US009129199B2

(12) **United States Patent**
Spodak et al.

(10) **Patent No.: US 9,129,199 B2**
(45) **Date of Patent: *Sep. 8, 2015**

(54) **PORTABLE E-WALLET AND UNIVERSAL CARD**

(71) Applicants: **Douglas A. Spodak**, Bala Cynwyd, PA (US); **Ron Fridman**, Paoli, PA (US)

(72) Inventors: **Douglas A. Spodak**, Bala Cynwyd, PA (US); **Ron Fridman**, Paoli, PA (US)

(73) Assignee: **GoNow Technologies, LLC**, Bound Brook, NJ (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 27 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/644,714**

(22) Filed: **Oct. 4, 2012**

(65) **Prior Publication Data**

US 2013/0030997 A1 Jan. 31, 2013

Related U.S. Application Data

(63) Continuation-in-part of application No. 13/438,131, filed on Apr. 3, 2012, which is a continuation-in-part of application No. 13/359,352, filed on Jan. 26, 2012, which is a continuation-in-part of application No. 13/310,491, filed on Dec. 2, 2011, which is a continuation-in-part of application No. 12/715,977, filed on Mar. 2, 2010.

(51) **Int. Cl.**
G06Q 40/00 (2012.01)
G06K 19/06 (2006.01)
(Continued)

(52) **U.S. Cl.**
CPC ***G06K 19/06187*** (2013.01); ***G06K 19/0718*** (2013.01); ***G06K 19/0723*** (2013.01); ***G06K 19/07707*** (2013.01); ***G06Q 20/3226*** (2013.01); ***G06Q 20/3278*** (2013.01); ***G06Q 20/341*** (2013.01); ***G06Q 20/347*** (2013.01); ***G06Q 20/352*** (2013.01); ***G06Q 20/3552*** (2013.01); ***G06Q 20/3572*** (2013.01); ***G06Q 20/363*** (2013.01); ***G06Q 20/367*** (2013.01);
(Continued)

(58) **Field of Classification Search**
USPC 705/41
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,491,725 A 1/1985 Pritchard
4,689,478 A 8/1987 Hale et al.
(Continued)

FOREIGN PATENT DOCUMENTS

WO WO 2005/086102 9/2005
WO WO 2007/028634 3/2007

OTHER PUBLICATIONS

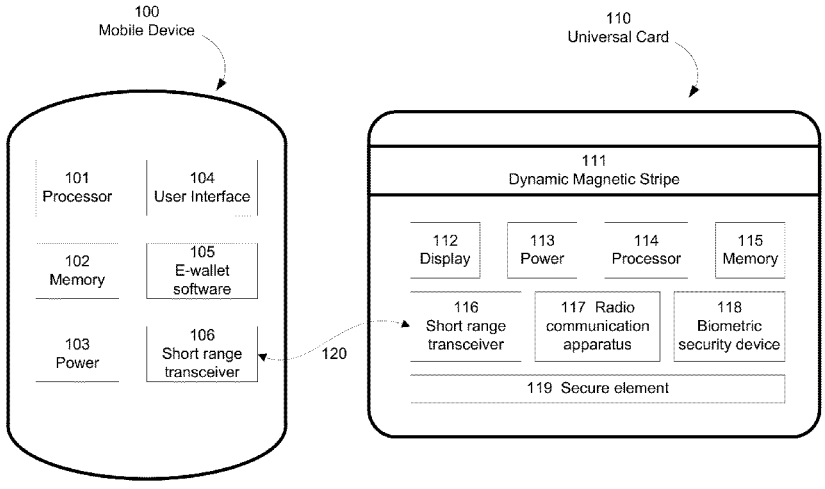
International Patent Application No. PCT/US2013/023149: International Search Report and Written Opinion dated Jun. 5, 2013, 40 pages.
(Continued)

Primary Examiner — Hani M Kazimi
Assistant Examiner — Hatem M Ali
(74) *Attorney, Agent, or Firm* — Baker & Hostetler LLP

(57) **ABSTRACT**

Universal cards are used in place of all the other traditional cards which a person may want to carry. The universal card can include a short range communications transceiver to communicate with a mobile device. The mobile device can include a user interface and an e-wallet application so that the user can interface with the e-wallet application for programming the universal card via the short range communication link. Once programmed, the universal card emulates a function of a traditional card.

32 Claims, 26 Drawing Sheets



(51) **Int. Cl.**

G06K 19/07	(2006.01)
G06K 19/077	(2006.01)
G06Q 20/36	(2012.01)
G06Q 20/32	(2012.01)
G06Q 20/34	(2012.01)
G07F 7/08	(2006.01)
G07F 7/10	(2006.01)

(52) **U.S. Cl.**

CPC ***G07F 7/086*** (2013.01); ***G07F 7/0846*** (2013.01); ***G07F 7/1008*** (2013.01)

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,276,311	A	1/1994	Hennige
5,590,038	A	12/1996	Pitroda
5,594,493	A	1/1997	Nemirofsky
5,748,737	A	5/1998	Daggar
5,884,271	A	3/1999	Pitroda
5,939,699	A	8/1999	Perttunen et al.
6,131,811	A	10/2000	Gangi
6,161,005	A	12/2000	Pinzon
6,336,098	B1	1/2002	Fortenberry et al.
6,607,136	B1	8/2003	Atsmon et al.
6,617,975	B1	9/2003	Burgess
6,641,050	B2	11/2003	Kelley et al.
6,715,679	B1	4/2004	Infosino
6,718,240	B1	4/2004	Suda et al.
6,736,322	B2	5/2004	Gobburu et al.
6,769,607	B1	8/2004	Pitroda et al.
6,785,595	B2	8/2004	Kominami et al.
6,925,439	B1	8/2005	Pitroda
6,967,562	B2	11/2005	Menard et al.
7,003,495	B1	2/2006	Burger et al.
7,097,108	B2	8/2006	Zellner et al.
7,128,274	B2	10/2006	Kelley et al.
7,152,783	B2	12/2006	Charrin
7,213,742	B1	5/2007	Birch et al.
7,343,317	B2	3/2008	Jokinen et al.
7,499,889	B2	3/2009	Golan et al.
7,591,416	B2	9/2009	Blossom
7,681,252	B1	3/2010	Petry
7,907,896	B2	3/2011	Chitti
8,082,575	B2	12/2011	Doughty et al.
8,200,582	B1	6/2012	Zhu
8,326,758	B2	12/2012	Bennett
2002/0004746	A1	1/2002	Ferber et al.
2002/0198777	A1	12/2002	Yuasa
2003/0055785	A1	3/2003	Lahiri
2003/0166400	A1	9/2003	Lucas
2004/0019564	A1*	1/2004	Goldthwaite et al. 705/44
2004/0159700	A1	8/2004	Khan et al.
2005/0021400	A1	1/2005	Postrel
2005/0101314	A1	5/2005	Levi
2005/0173519	A1	8/2005	Gatto
2005/0194452	A1	9/2005	Nordentoft et al.
2006/0081702	A1	4/2006	Nandakumar
2006/0190412	A1	8/2006	Ostroff
2007/0045401	A1	3/2007	Sturm
2007/0189581	A1	8/2007	Nordentoft et al.
2007/0252010	A1	11/2007	Gonzalez et al.
2007/0254712	A1*	11/2007	Chitti 455/558
2007/0278291	A1	12/2007	Rans et al.
2007/0288313	A1	12/2007	Brodson et al.
2008/0059379	A1	3/2008	Ramaci et al.
2008/0120186	A1	5/2008	Jokinen et al.
2008/0147546	A1	6/2008	Weichselbaumer et al.
2009/0103732	A1	4/2009	Benteo et al.
2009/0199206	A1	8/2009	Finkenzeller et al.
2009/0261166	A1	10/2009	Lawson et al.
2010/0057580	A1	3/2010	Raghunathan
2010/0280948	A1	11/2010	Cohen
2011/0062242	A1	3/2011	Cowcher
2011/0140841	A1	6/2011	Bona et al.
2011/0218911	A1	9/2011	Spodak
2011/0219026	A1	9/2011	Schonemann
2012/0074232	A1	3/2012	Spodak
2012/0123937	A1	5/2012	Spodak
2012/0191612	A1	7/2012	Spodak et al.

OTHER PUBLICATIONS

International Patent Application No. PCT/US2011/63319: International Search Report and Written Opinion dated Apr. 25, 2012, 15 pages.

Smart cards: Anonymous; Retail Delivery strategies 9 (1998):5-27.

Smart cards Do not have all the answers: Motoco Rich and Gerge Graham Financial Times. Financial Post [Toronto,Ont] Aug. 27, 1996:53.

AT & T joins banks in Mondex line-up: Anonymous. Financial Technology International Bulletin 13.12 (Aug. 1996): 1.

* cited by examiner

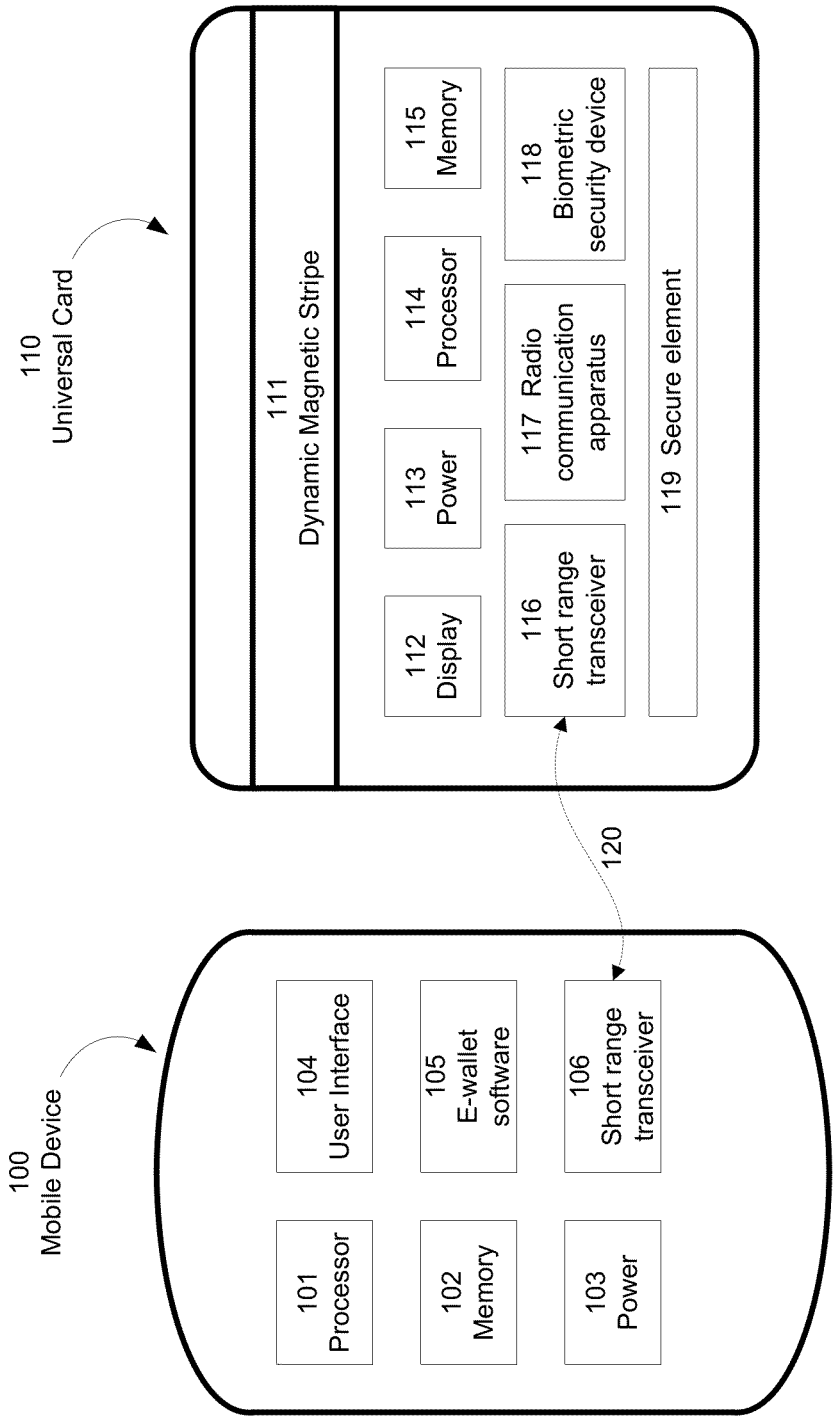

100
Mobile Device
101
Processor
102
Memory
103
Power
104
User Interface
105
E-wallet
software
106
Short range
transceiver
120
110
Universal Card
111
Dynamic Magnetic Stripe
112
Display
113
Power
114
Processor
115
Memory
116
Short range
transceiver
117 Radio
communication
apparatus
118
Biometric
security device
119 Secure element

FIGURE 1

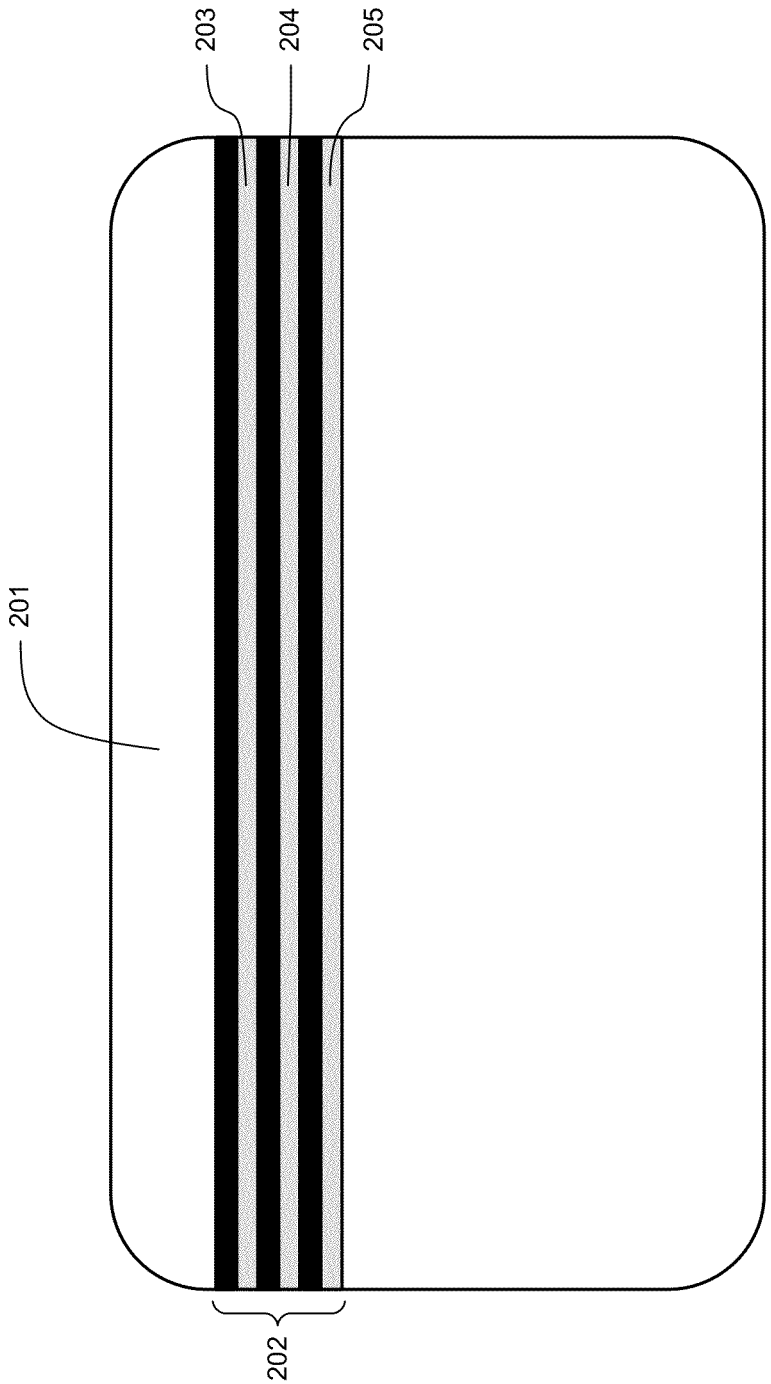


FIGURE 2

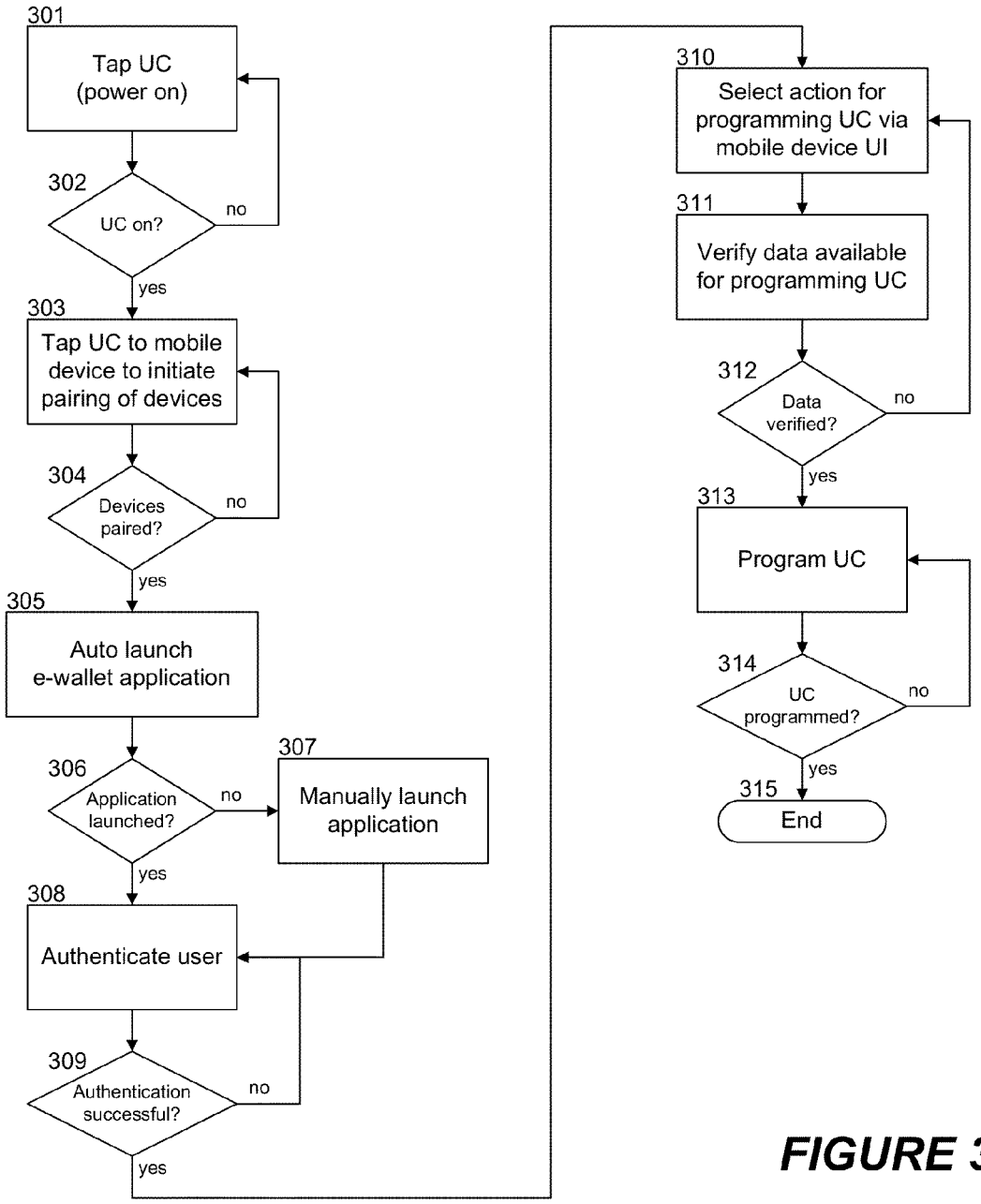

301
Tap UC (power on)
302
UC on?
no
yes
303
Tap UC to mobile device to initiate pairing of devices
304
Devices paired?
no
yes
305
Auto launch e-wallet application
306
Application launched?
no
307
Manually launch application
yes
308
Authenticate user
309
Authentication successful?
no
yes
310
Select action for programming UC via mobile device UI
311
Verify data available for programming UC
312
Data verified?
no
yes
313
Program UC
314
UC programmed?
no
yes
315
End

FIGURE 3

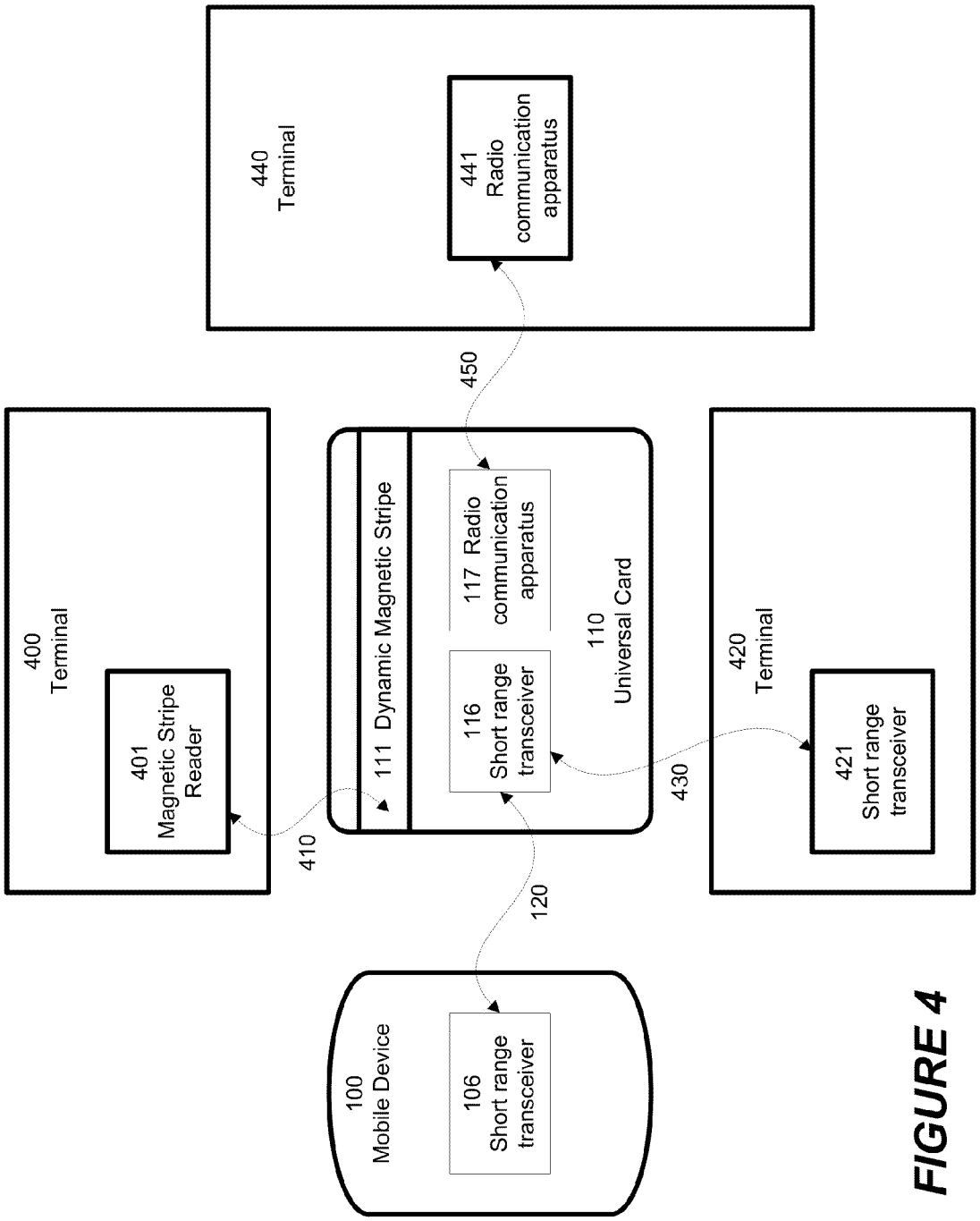

440
Terminal
441
Radio
communication
apparatus
450
400
Terminal
401
Magnetic Stripe
Reader
410
111 Dynamic Magnetic Stripe
117 Radio
communication
apparatus
116
Short range
transceiver
110
Universal Card
430
420
Terminal
421
Short range
transceiver
120
100
Mobile Device
106
Short range
transceiver

FIGURE 4

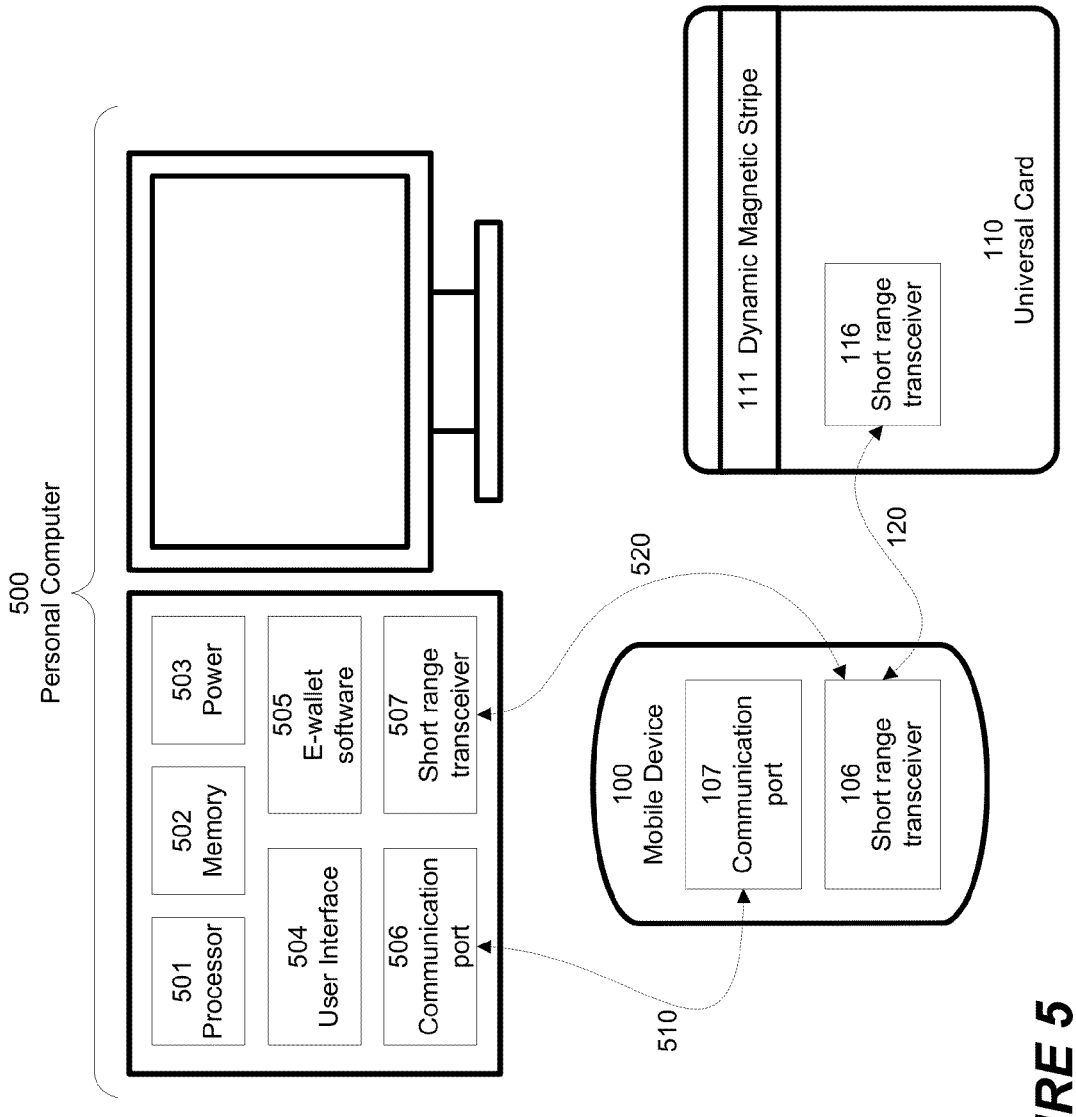

500
Personal Computer
501 Processor
502 Memory
503 Power
504 User Interface
505 E-wallet software
506 Communication port
507 Short range transceiver
510
520
100 Mobile Device
107 Communication port
106 Short range transceiver
120
111 Dynamic Magnetic Stripe
116 Short range transceiver
110 Universal Card

FIGURE 5

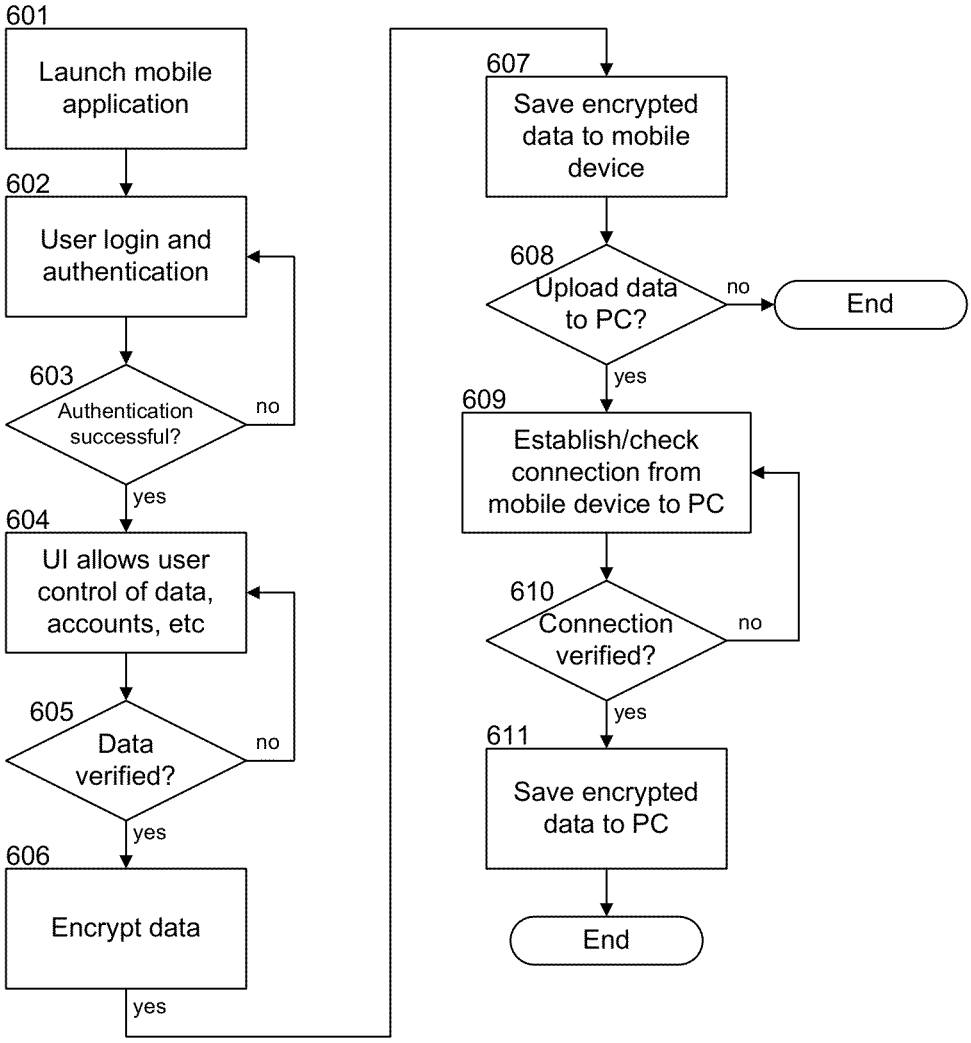

601
Launch mobile application
602
User login and authentication
603
Authentication successful?
no
yes
604
UI allows user control of data, accounts, etc
605
Data verified?
no
yes
606
Encrypt data
yes
607
Save encrypted data to mobile device
608
Upload data to PC?
no
End
yes
609
Establish/check connection from mobile device to PC
610
Connection verified?
no
yes
611
Save encrypted data to PC
End

FIGURE 6

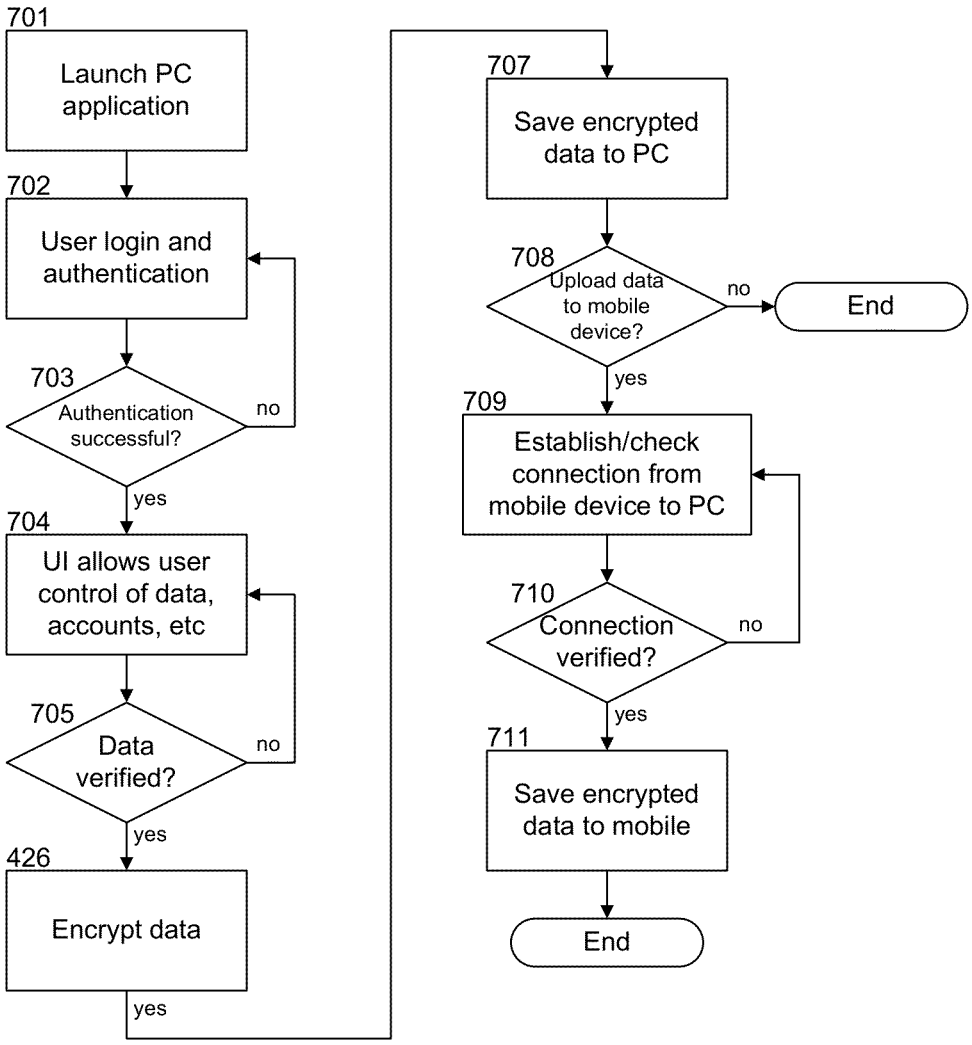

701
Launch PC application
702
User login and authentication
703
Authentication successful?
no
yes
704
UI allows user control of data, accounts, etc
705
Data verified?
no
yes
426
Encrypt data
yes
707
Save encrypted data to PC
708
Upload data to mobile device?
no
End
yes
709
Establish/check connection from mobile device to PC
710
Connection verified?
no
yes
711
Save encrypted data to mobile
End

FIGURE 7

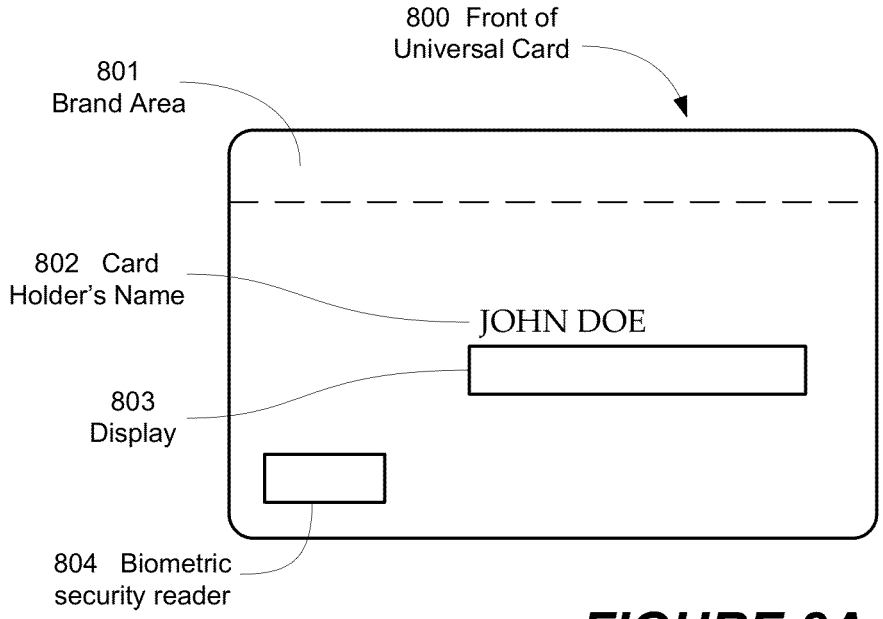


FIGURE 8A

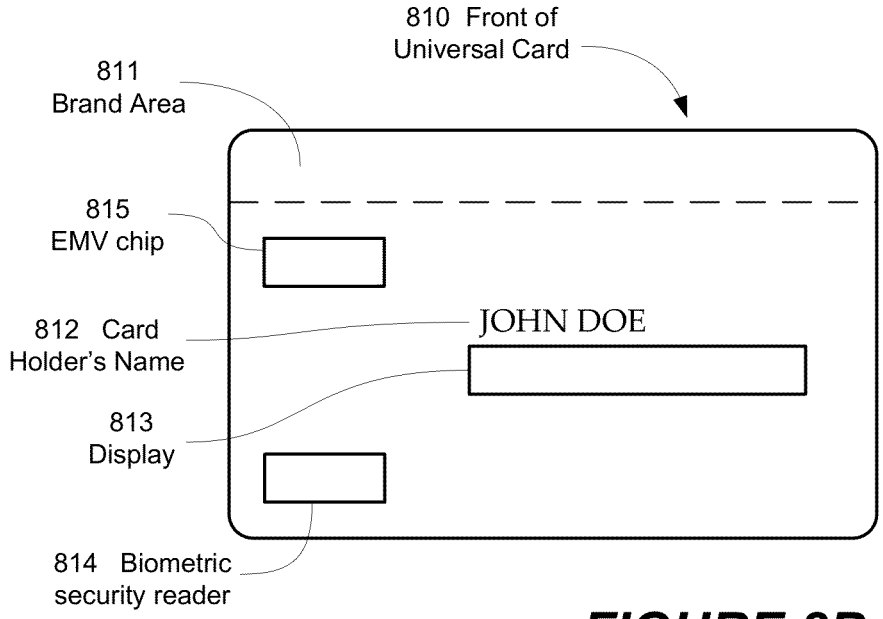


FIGURE 8B

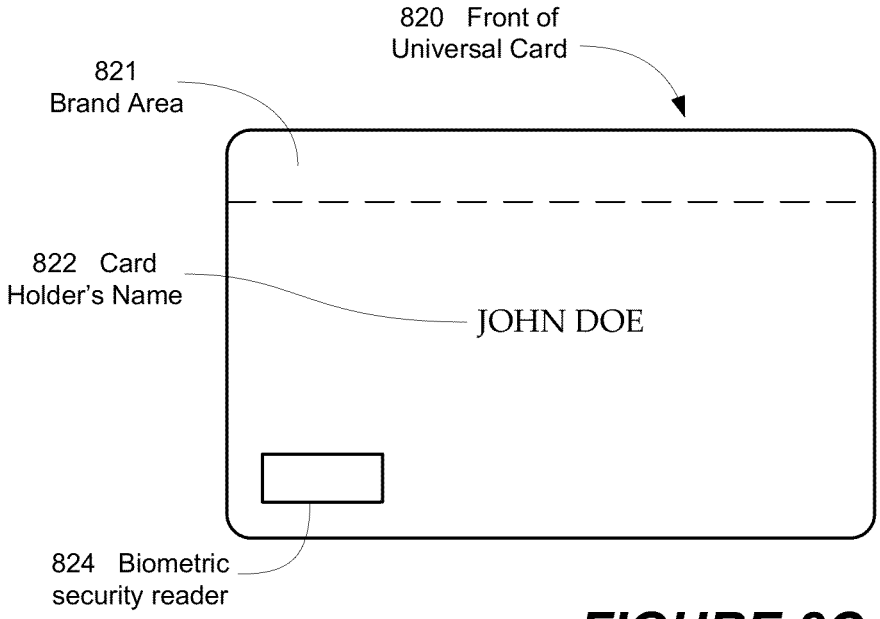


FIGURE 8C

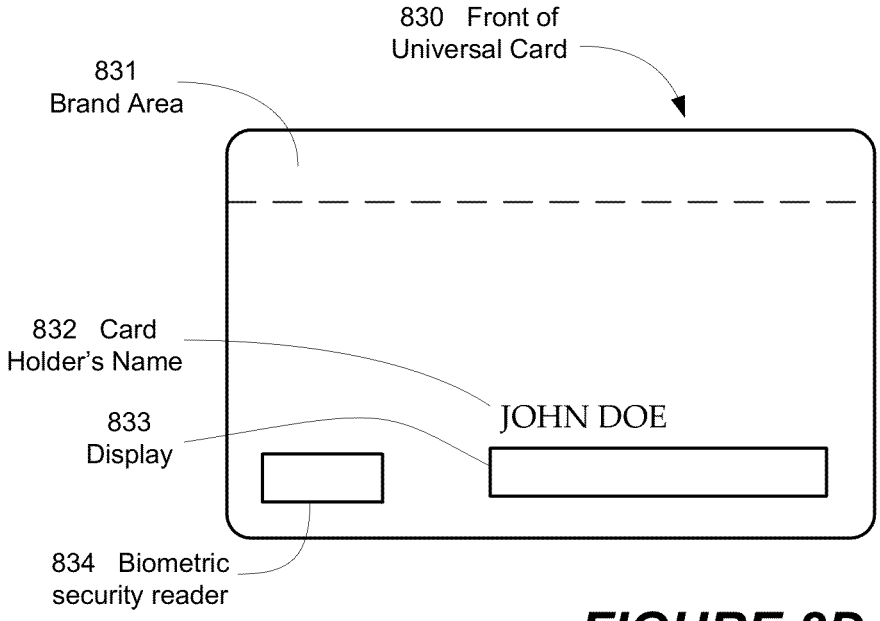


FIGURE 8D

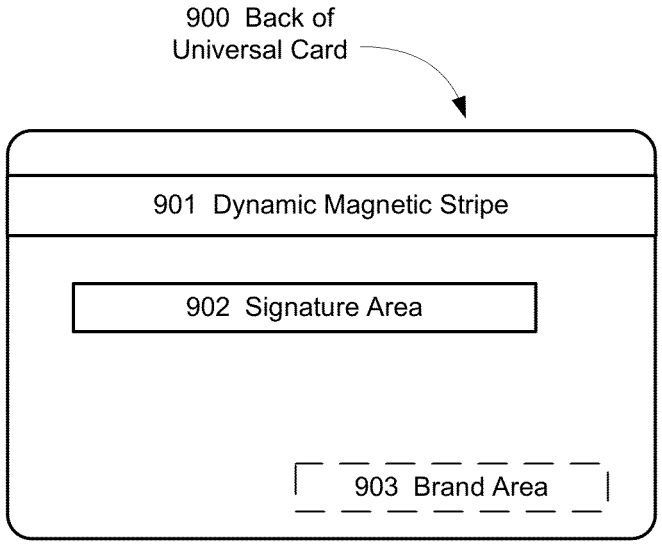

900 Back of
Universal Card
901 Dynamic Magnetic Stripe
902 Signature Area
903 Brand Area

FIGURE 9

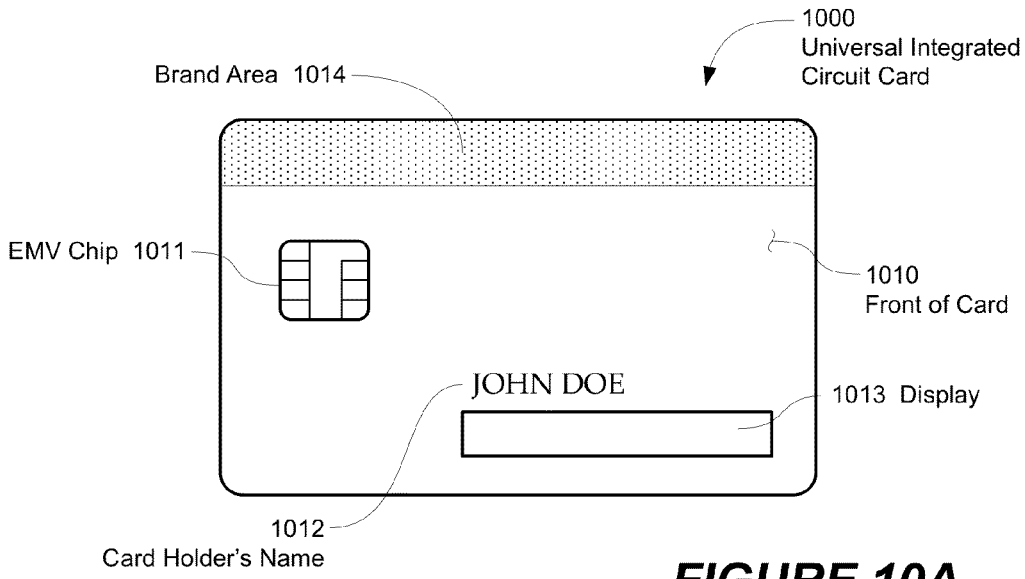


FIGURE 10A

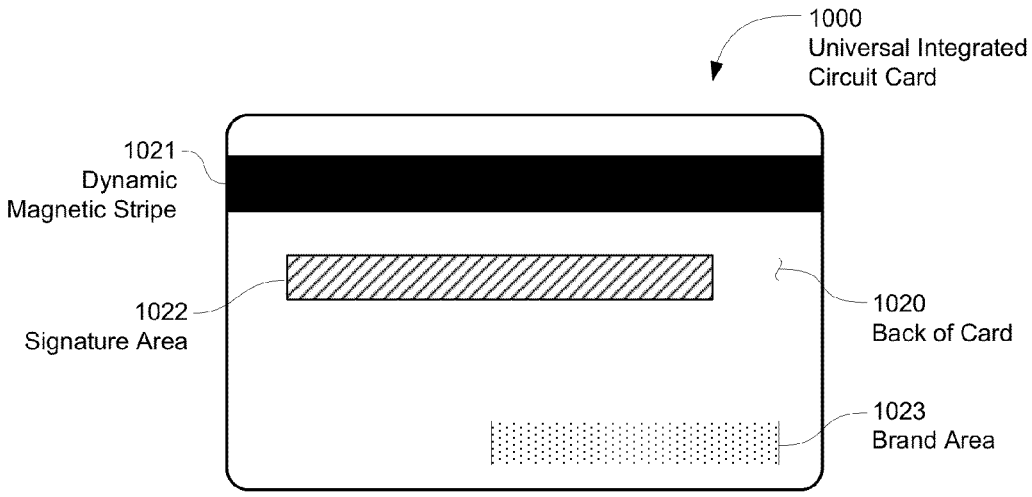


FIGURE 10B

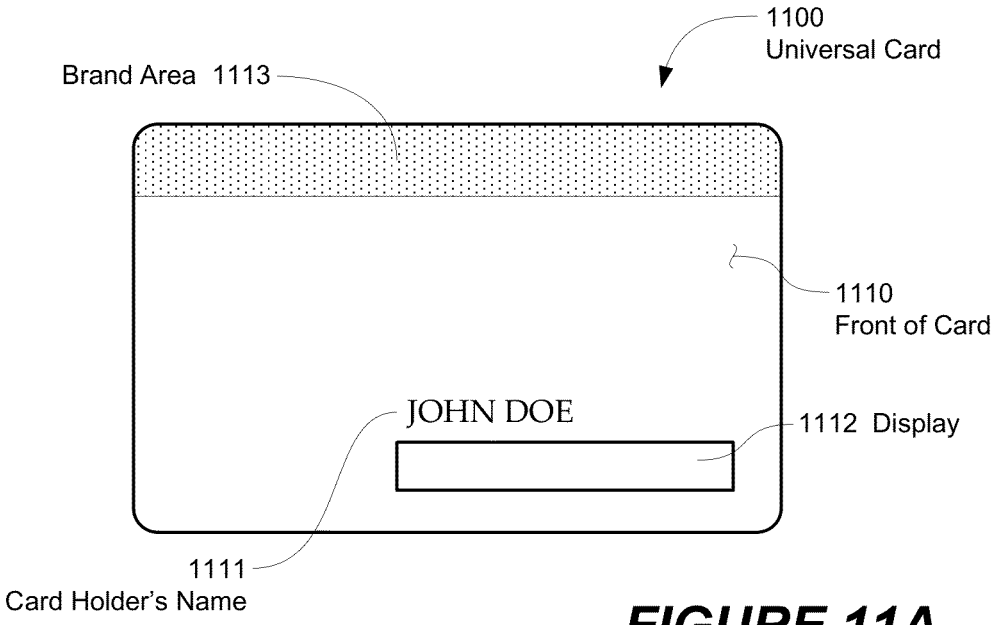


FIGURE 11A

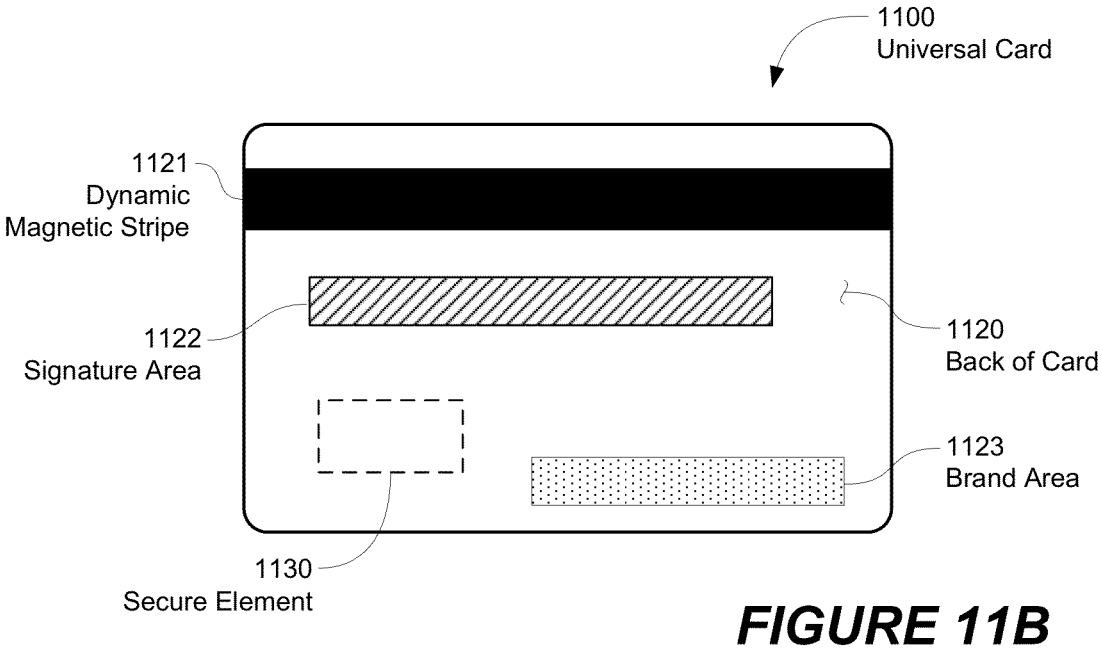


FIGURE 11B

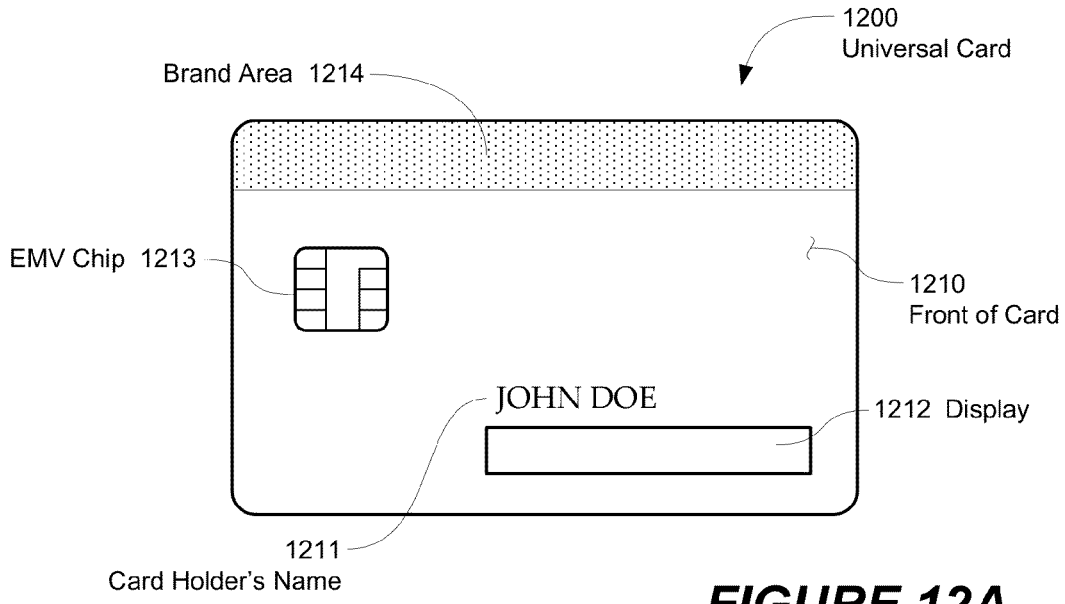


FIGURE 12A

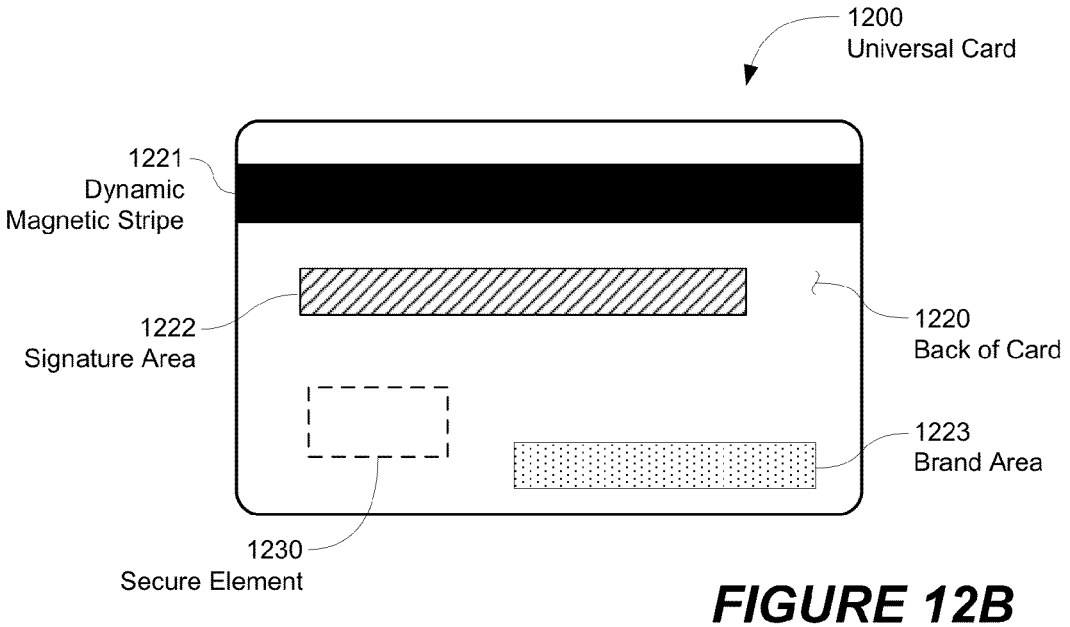


FIGURE 12B

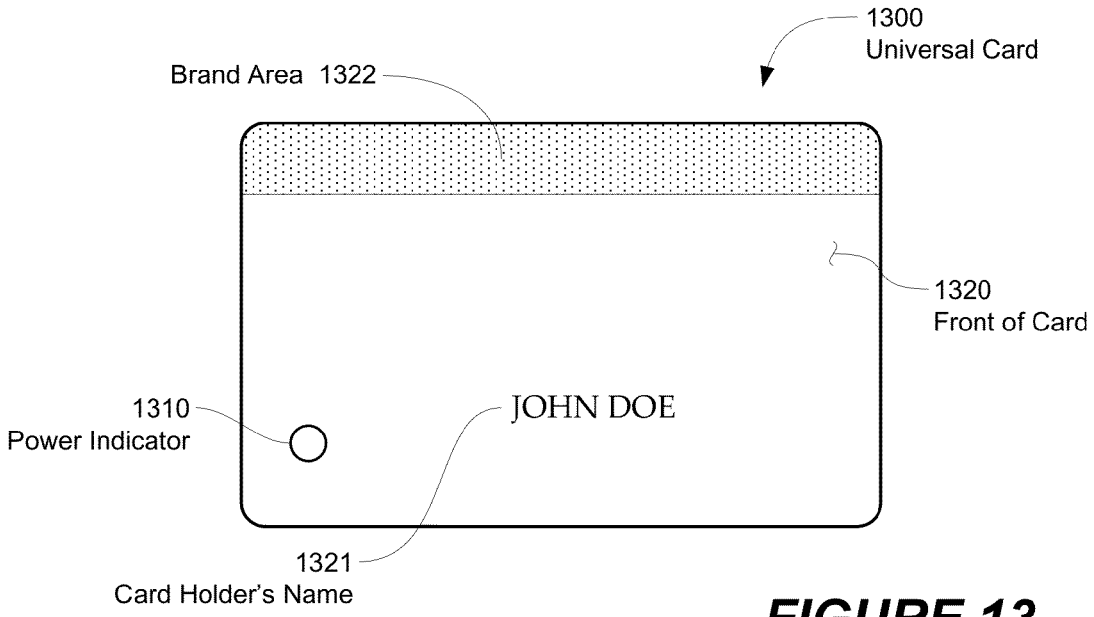


FIGURE 13

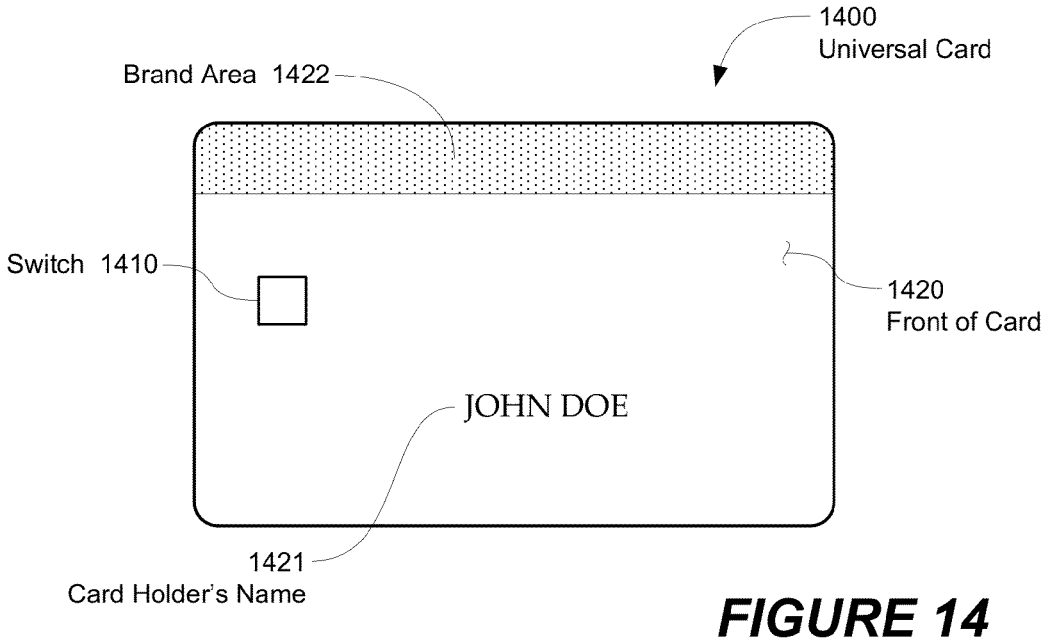


FIGURE 14

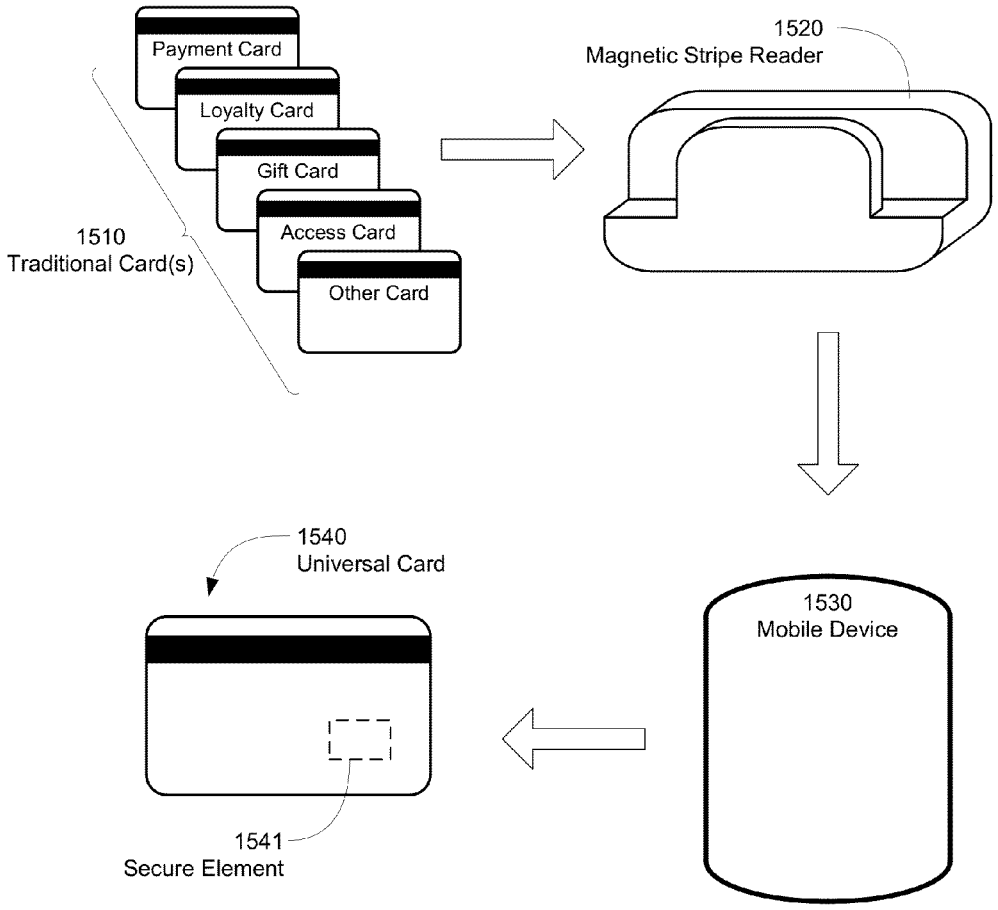

Payment Card
Loyalty Card
Gift Card
Access Card
Other Card
1510
Traditional Card(s)
1520
Magnetic Stripe Reader
1530
Mobile Device
1540
Universal Card
1541
Secure Element

FIGURE 15A

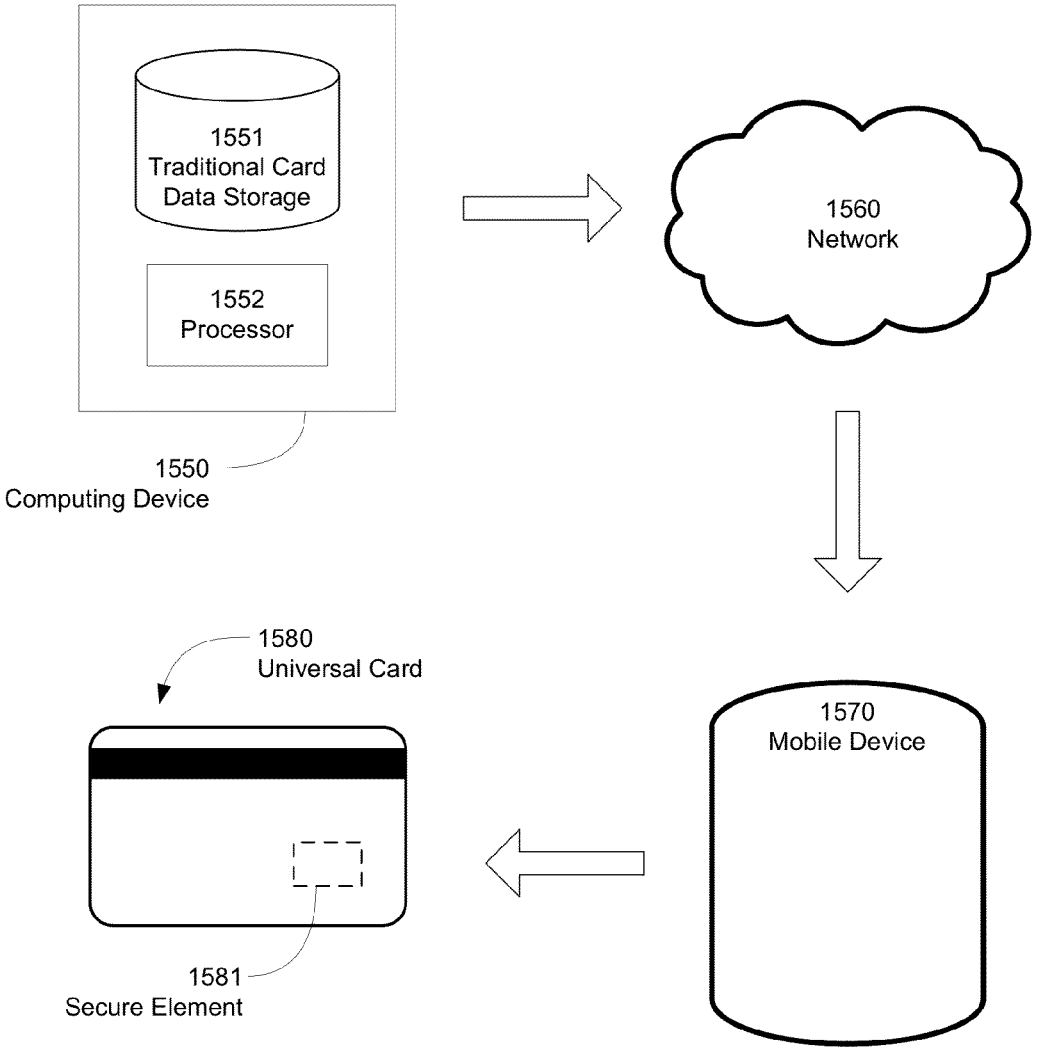

1551
Traditional Card
Data Storage
1552
Processor
1550
Computing Device
1560
Network
1570
Mobile Device
1580
Universal Card
1581
Secure Element

FIGURE 15B

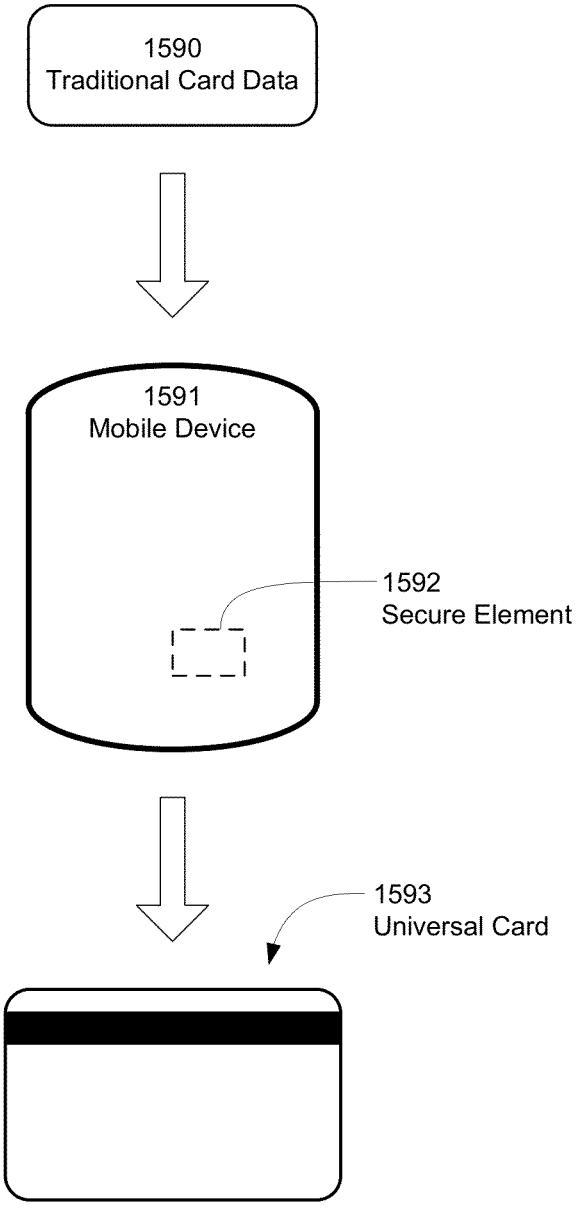

1590
Traditional Card Data
1591
Mobile Device
1592
Secure Element
1593
Universal Card

FIGURE 15C

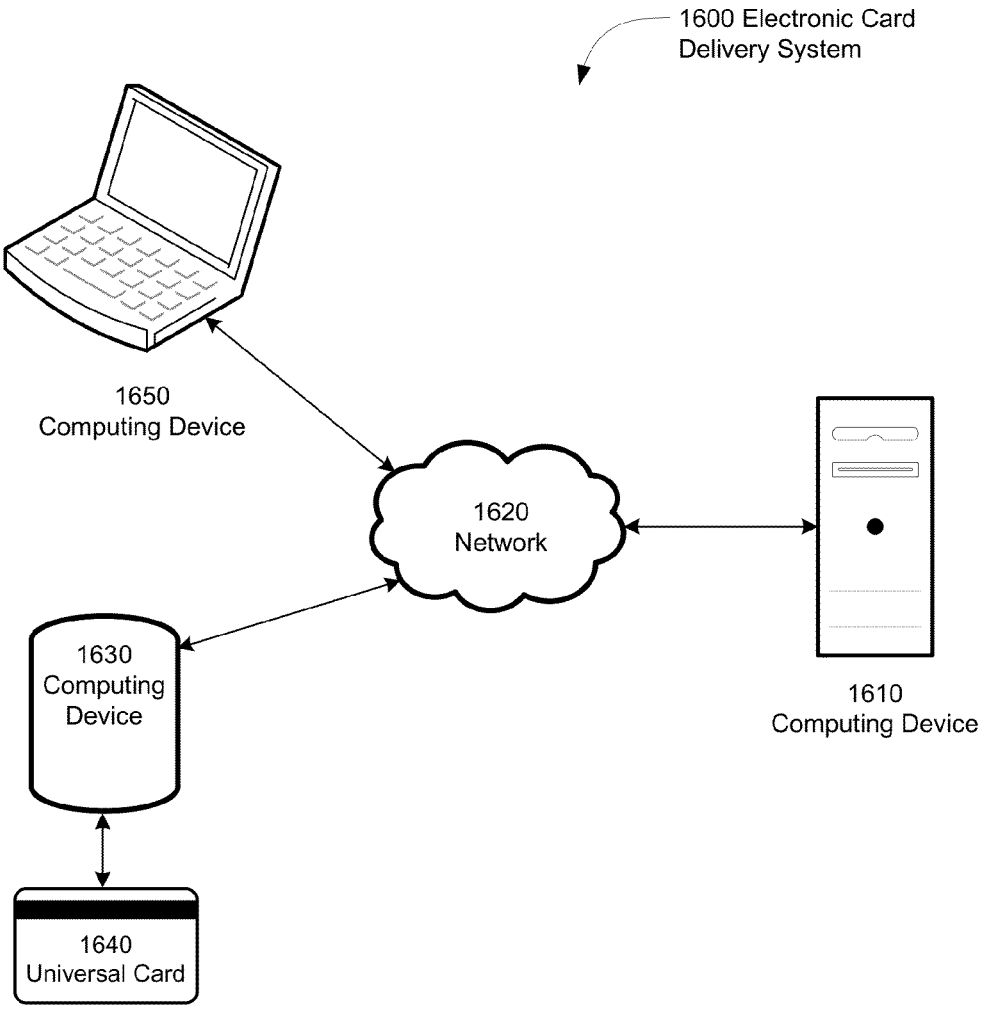

1600 Electronic Card Delivery System
1650 Computing Device
1620 Network
1610 Computing Device
1630 Computing Device
1640 Universal Card

FIGURE 16

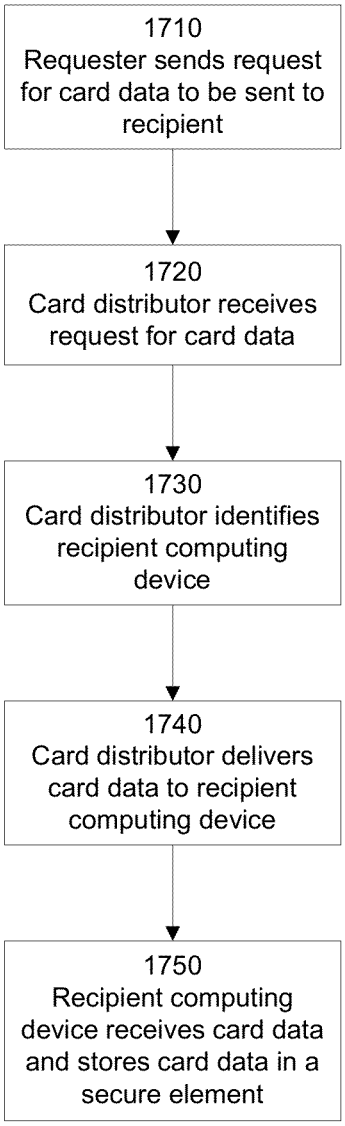

1710
Requester sends request for card data to be sent to recipient
1720
Card distributor receives request for card data
1730
Card distributor identifies recipient computing device
1740
Card distributor delivers card data to recipient computing device
1750
Recipient computing device receives card data and stores card data in a secure element

FIGURE 17

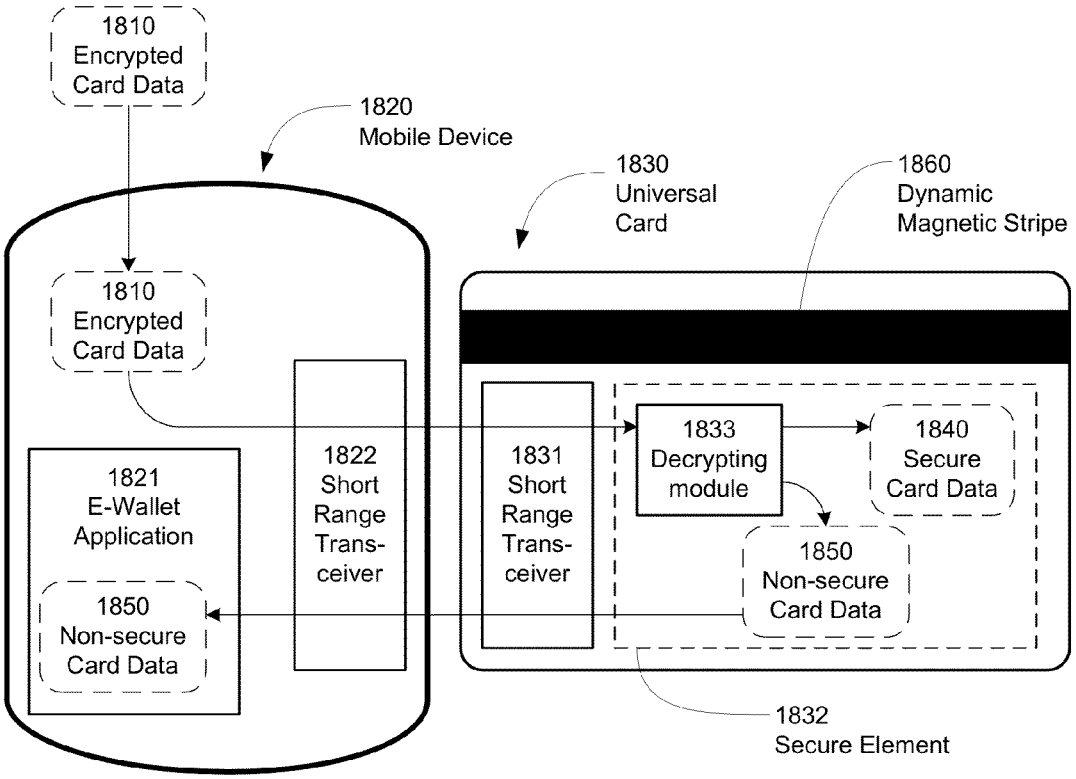

1810
Encrypted
Card Data
1820
Mobile Device
1830
Universal
Card
1860
Dynamic
Magnetic Stripe
1810
Encrypted
Card Data
1821
E-Wallet
Application
1850
Non-secure
Card Data
1822
Short
Range
Trans-
ceiver
1831
Short
Range
Trans-
ceiver
1833
Decrypting
module
1840
Secure
Card Data
1850
Non-secure
Card Data
1832
Secure Element

FIGURE 18

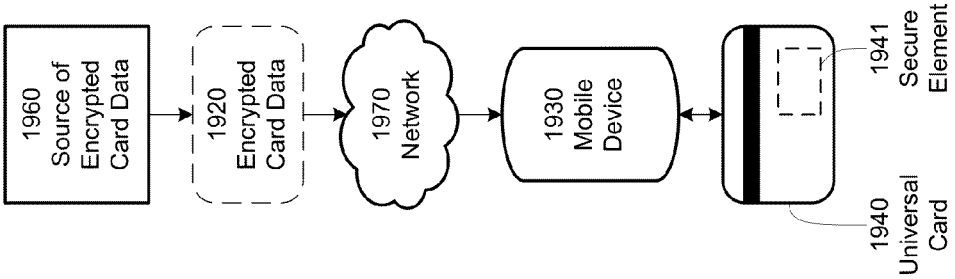


FIGURE 19C

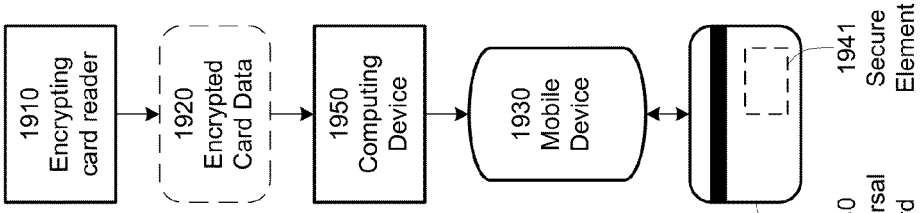


FIGURE 19B

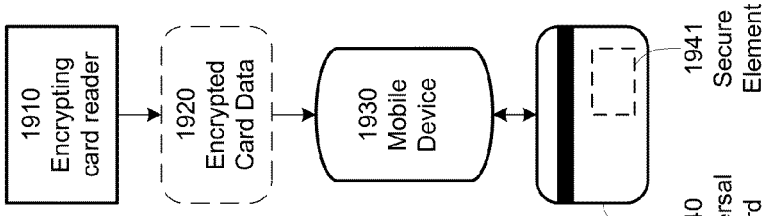


FIGURE 19A

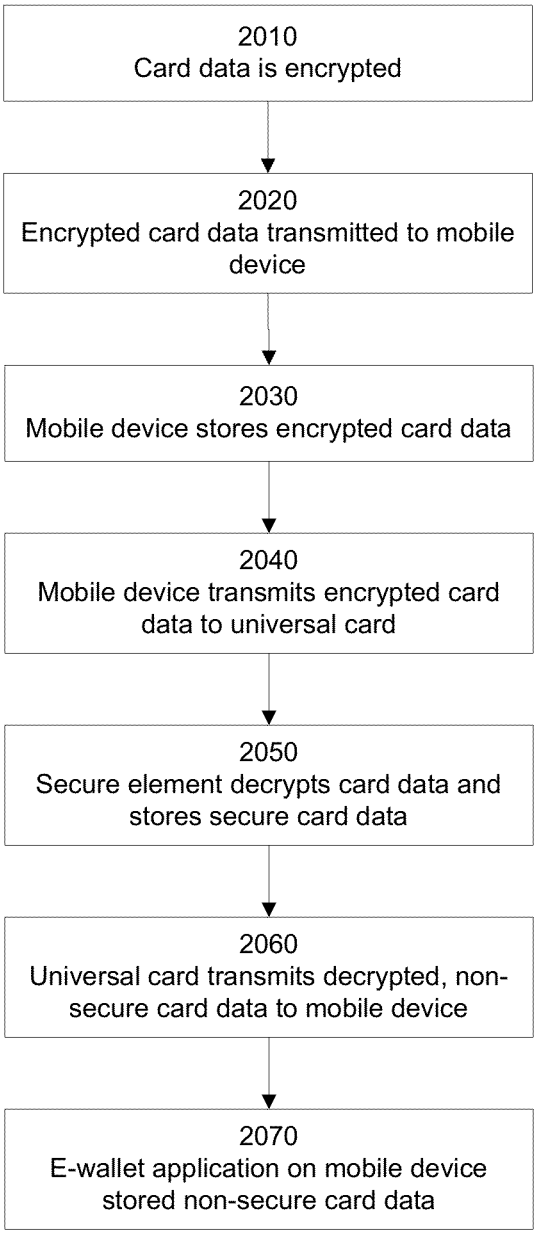

2010
Card data is encrypted
2020
Encrypted card data transmitted to mobile device
2030
Mobile device stores encrypted card data
2040
Mobile device transmits encrypted card data to universal card
2050
Secure element decrypts card data and stores secure card data
2060
Universal card transmits decrypted, non-secure card data to mobile device
2070
E-wallet application on mobile device stored non-secure card data

FIGURE 20

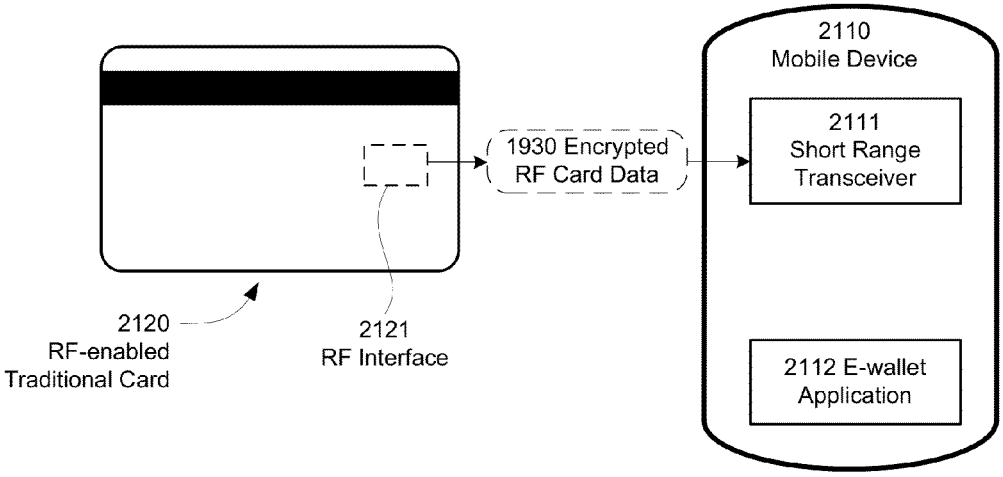


FIGURE 21A

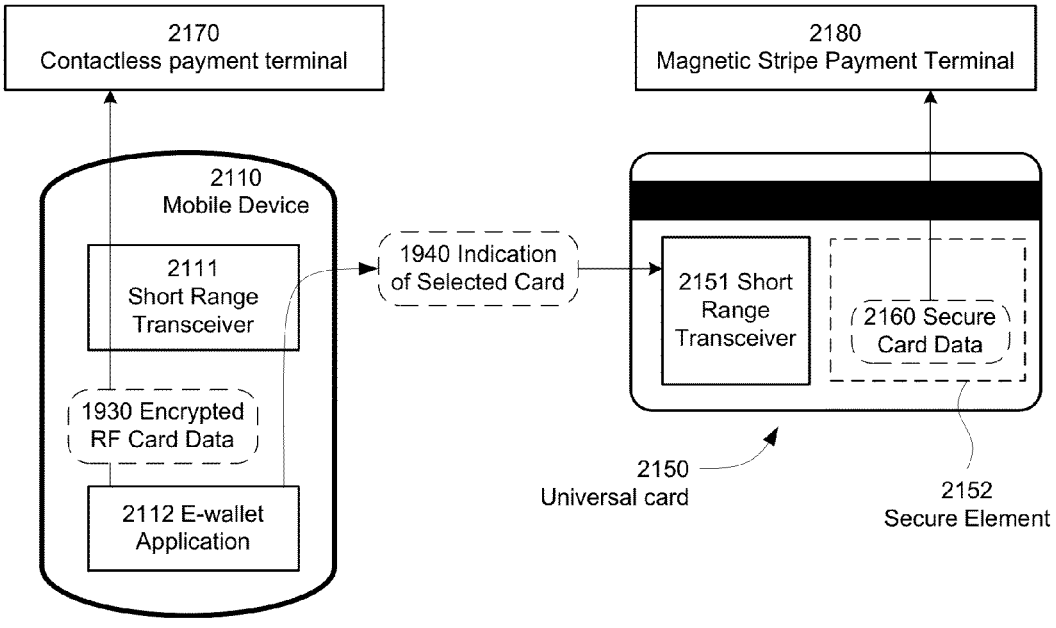


FIGURE 21B

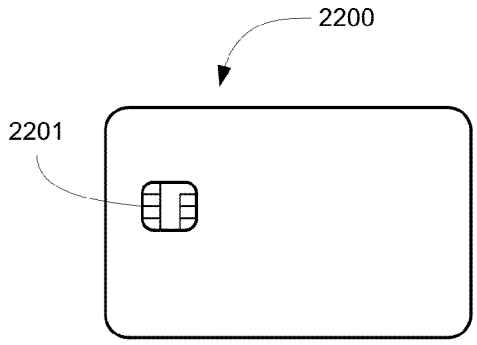


FIGURE 22A

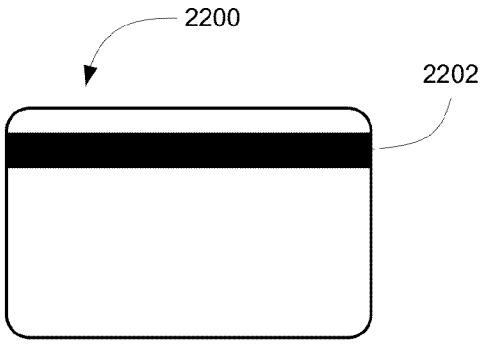


FIGURE 22B

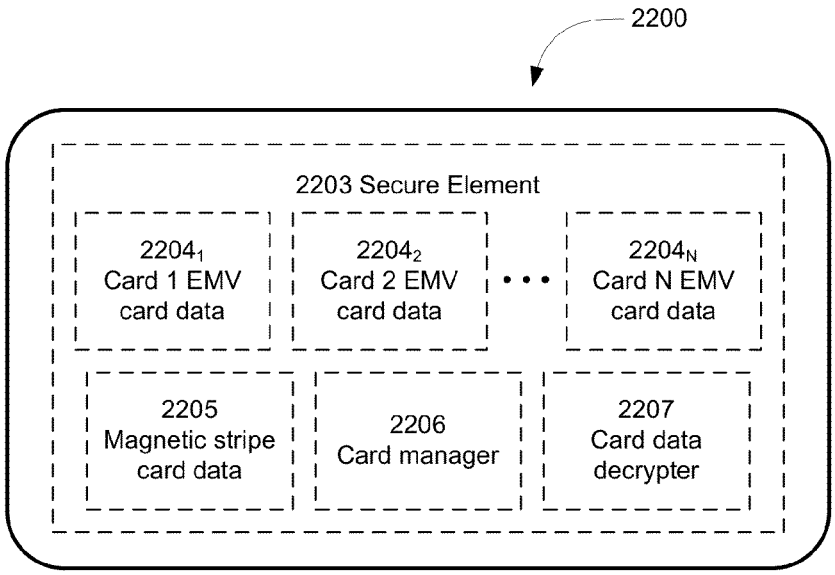


FIGURE 22C

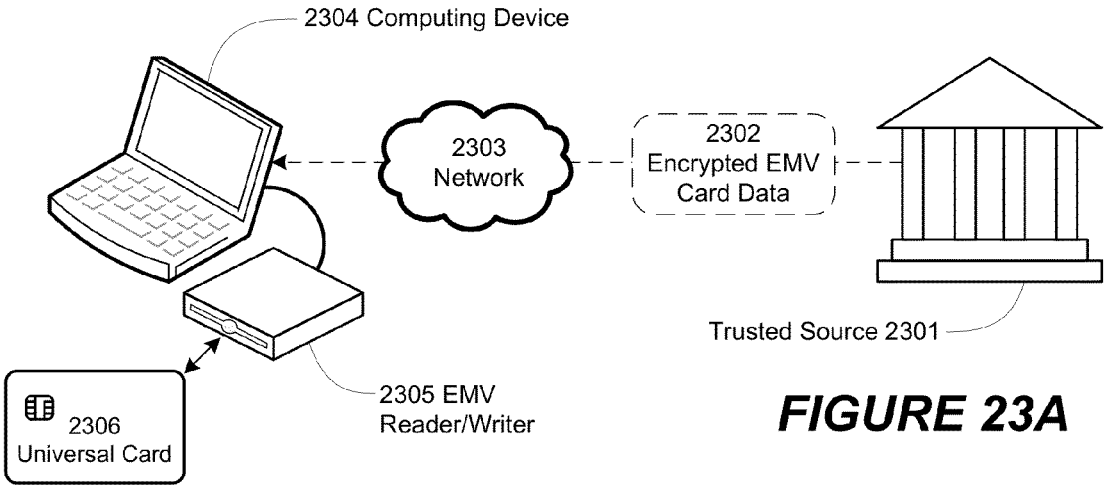


FIGURE 23A

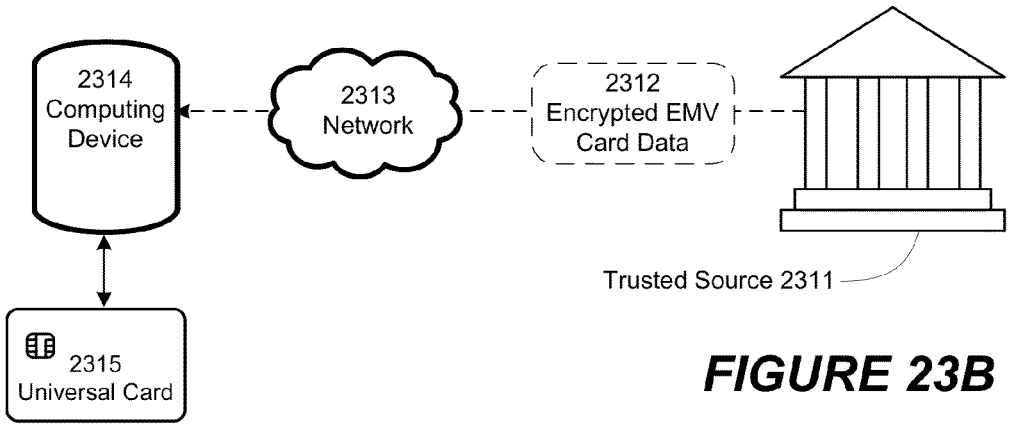


FIGURE 23B

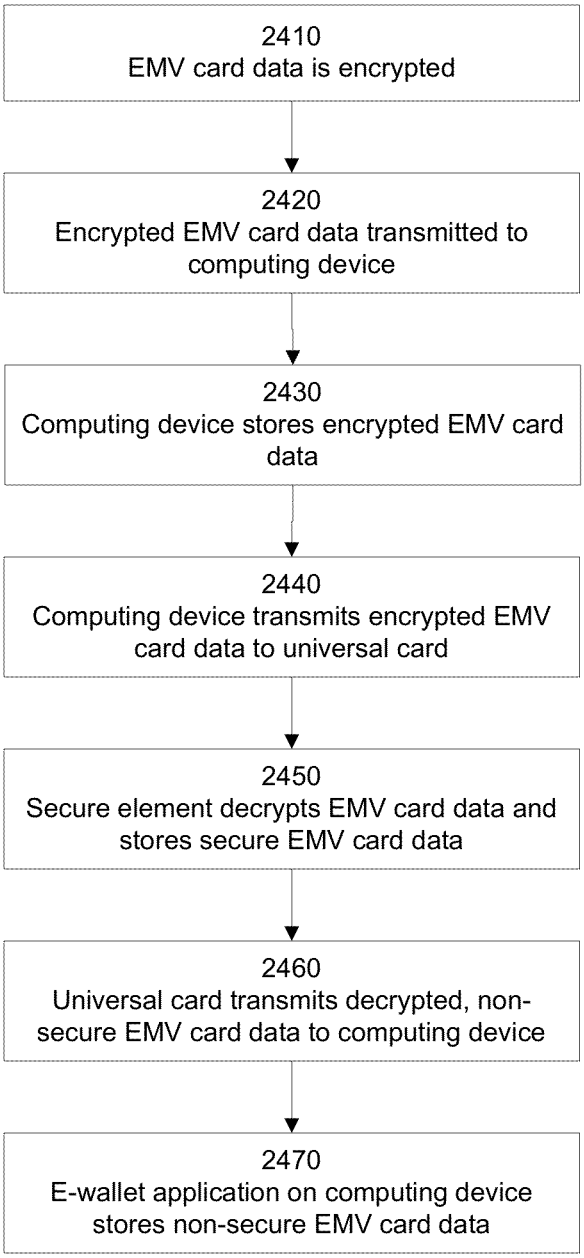

2410
EMV card data is encrypted
2420
Encrypted EMV card data transmitted to computing device
2430
Computing device stores encrypted EMV card data
2440
Computing device transmits encrypted EMV card data to universal card
2450
Secure element decrypts EMV card data and stores secure EMV card data
2460
Universal card transmits decrypted, non-secure EMV card data to computing device
2470
E-wallet application on computing device stores non-secure EMV card data

FIGURE 24

PORTABLE E-WALLET AND UNIVERSAL CARD

CROSS REFERENCE TO RELATED APPLICATION

This application is a continuation-in-part of U.S. patent application Ser. No. 13/438,131 filed Apr. 3, 2012, which is a continuation-in-part of U.S. patent application Ser. No. 13/359,352 filed Jan. 26, 2012, which is a continuation-in-part of U.S. patent application Ser. No. 13/310,491 filed Dec. 2, 2011, which is a continuation-in-part of U.S. patent application Ser. No. 12/715,977 filed Mar. 2, 2010. The contents of each are herein incorporated by reference in their entirety.

TECHNICAL FIELD

The presently disclosed subject matters relates to universal cards, mobile applications, and mobile devices such as mobile phones, Personal Digital Assistants (PDAs), iPods, tablet computers, laptop computers, and similar mobile devices. More particularly, the subject matter relates to a universal card which can be used at any type of terminal equipped with a magnetic stripe reader or a short range wireless communication capability.

BACKGROUND

People carry many types of cards with them every day. The cards include credit cards, debit cards, drivers' licenses, transportation passes, building access cards, and many other types of cards. These cards are typically carried in a wallet or purse. A person may need to use any number of cards during the course of a day. Since people do not know which of the cards will be needed on any given day, most people carry all the cards that they may need with them every day. With the proliferation of card-capable terminals, people can end up carrying an inordinate amount of cards with them every day.

Many people also carry mobile devices with them, such as cell phones, PDAs, tablet computers, laptop computers, and many other types of mobile devices. Mobile devices increasingly have short range communication capabilities, such as near field communication (NFC) capabilities or Bluetooth capabilities.

A person that carries a wallet or purse also has to secure the contents of the wallet or purse at all times to protect against theft and fraud. If a card is lost or stolen, it can be used in unauthorized ways, leading to identification theft, fraud, or financial loss. In addition, as many transactions are increasingly performed without the need for physically possessing the card (e.g., online purchases), the mere exposure of the information found on a card to an unauthorized person is a risk to the card holder.

There is a need to reduce the number of cards carried by a person, and an opportunity to address that need using the short range communication capabilities of a mobile device which that person carries. In addition, there is a need to secure cards and card information so that cards and card information is not exposed to unauthorized people.

SUMMARY

To reduce the number of cards carried by a person, a universal card and short range communication enabled mobile device can be used in place of all the other cards which the person may want to carry. The universal card can include a short range communications transceiver to communicate with a mobile device. The mobile device can include a user interface and an e-wallet application so that the user can interface with the e-wallet application for programming the universal card via the short range communication link. Once programmed, the universal card emulates a function of a traditional card, such as emulating the magnetic stripe of the traditional card, the NFC communication of the traditional card, the radio transmission of the traditional card, or any other function.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing Summary, as well as the following Detailed Description, is better understood when read in conjunction with the appended drawings. In order to illustrate the present disclosure, various aspects of the disclosure are shown. However, the disclosure is not limited to the specific aspects shown. The following figures are included:

FIG. **1** depicts an exemplary system including a mobile device and a universal card.

FIG. **2** depicts a traditional card with a static magnetic stripe.

FIG. **3** depicts a flowchart process for programming a universal card.

FIG. **4** depicts interactions between a mobile device and a universal card, and between a universal card and three different types of terminals.

FIG. **5** depicts an exemplary system including a personal computer, a mobile device, and a universal card.

FIG. **6** depicts a flowchart process for managing universal card data using a mobile device.

FIG. **7** depicts a flowchart process for managing universal card data using a personal computer.

FIGS. **8**A, **8**B, **8**C, and **8**D depict possible designs for the front of a universal card.

FIG. **9** depicts a possible design for the back of a universal card.

FIGS. **10**A and **10**B depict an embodiment of a universal card with an integrated circuit.

FIGS. **11**A and **11**B depict an embodiment of a universal card with a secure element.

FIGS. **12**A and **12**B depict an embodiment of a universal card with an integrated circuit and a secure element.

FIG. **13** depicts an embodiment of a universal card with a power indicator.

FIG. **14** depicts an embodiment of a universal card with an activation switch.

FIGS. **15**A and **15**B depict ways to add traditional card data to a secure element of a universal card.

FIG. **15**C depicts a way to add traditional card data to a secure element of a mobile device.

FIG. **16** depicts an exemplary electronic card data delivery system.

FIG. **17** depicts an exemplary method of providing card data to a universal card.

FIG. **18** depicts embodiments of a system and method of securely loading card data onto a universal card that has a secure element

FIGS. **19**A, **19**B, and **19**C depict several embodiments of systems and methods for providing card encrypted to a mobile device for transmission to a universal card with a secure element.

FIG. **20** depicts an embodiment of a method of securely transferring secure card data to a universal card and non-secure card data to a mobile device.

FIGS. **21**A and **21**B depict embodiments of a mobile device obtaining and using RF card data in conjunction with a universal card.

FIGS. **22**A to **22**C depict an embodiment of a universal card with a dynamic EMV chip.

FIGS. **23**A and **23**B depict embodiments of storing EMV card data in a universal card.

FIG. **24** depicts an embodiment of a method of handling encrypted EMV card data by a computing device and a universal card.

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

Referring to FIG. **1**, an exemplary system is depicted with a mobile device **100** and a universal card **110**. The mobile device **100** can be any number of devices, including a cell phone, a PDA, an iPod, a tablet computer, an NFC-specialized device, or any other type of mobile device. An NFC-specialized device is a device that provides for the user to be able to communicate with NFC terminals, such as making a contactless payment, and would also provide a user with a user interface for interacting with an NFC-enabled universal card. The mobile device **100** may include any number of components, such as a processor **101**, memory **102**, a power source **103**, a user interface **104**, and a short range transceiver **106**. Memory **102** can be any type of computer storage media in the form of volatile and/or nonvolatile memory such as read only memory (ROM) and random access memory (RAM). Processor **101** can operate on data and/or software applications available in the memory **102**. The user interface **104** can include any components for user input, such as a keyboard, a mouse, a trackball, a touch screen display, or any similar component. The user interface **104** can also include security features on the mobile device, such as a PIN/password login, a fingerprint scanner, other biometric readers, or similar security features.

The mobile device **100** also includes an e-wallet application **105** which is executable by the processor **101**. The e-wallet application **105** can be pre-installed on the mobile device **100** by the manufacturer of the mobile device **100**. The e-wallet application **105** can also be installed by the user either by downloading it directly to the mobile device **100**, by downloading the e-wallet application **105** over-the-air via a wireless data connection, or by inserting a memory card containing the e-wallet application **105**.

The e-wallet application **105** allows the user to input information about traditional cards for storage in the memory **102**. Information about traditional cards can include an account name, an account number, an expiration date, a card verification value 2 (CVV2), the image of the traditional card, the information which would be stored on the magnetic stripe of the traditional card, and any other information necessary to emulate the card. The information about traditional cards can also be stored in a remote location, such as a trusted service manager (not shown), which stores the information and provides the information to the mobile device **100** on demand via wireless data communication. In this case, the e-wallet application **105** would interface with the remote location to request and receive the information.

The e-wallet application **105** can also be used to program the universal card **110** by allowing the user to select a traditional card for the universal card to emulate. The universal card **110** can be configured to emulate any number of traditional cards, including credit cards, debit cards, drivers' licenses, transportation passes, building access cards, and any other types of cards. Once the user selects a card for emulation, the e-wallet application **105** causes the mobile device to communicate with the universal card and to transmit the information necessary for the universal card to emulate the selected traditional card.

In another universal card embodiment, the information about the traditional card could be stored in the memory **115** of the universal card **110**. In this embodiment, if the universal card **110** has a user interface with sufficient capabilities, the user may be able to program the card by using the user interface on the universal card **110**.

The short range transceiver **106** can be configured to communicate via any type of short range communication link, such as an NFC communication link or a Bluetooth communication link. The mobile device **100** may be manufactured with the short range transceiver **106**. However, not all mobile devices are initially manufactured with short range transceivers. The short range transceiver **106** may be located on a memory card compatible with a memory slot of the mobile device **100**. In this situation, the memory card with the short range transceiver **106** is inserted into the memory slot (not shown) of the mobile device **100** such that the mobile device can transmit and receive information using a short range communication link corresponding to the short range transceiver **106**.

Another issue with the short range transceiver **106** may arise if the short range transceiver **106** of the mobile device and the short range transceiver **116** of the universal card **110** are not configured for the same type of short range communication. For example, mobile device **100** may have a Bluetooth transceiver, and the universal card **110** may have an NFC transceiver. In such a situation, the short range transceiver **106** would be a two-type transceiver, capable of communicating via both types of short range communication. In the example above, the short range transceiver **106** would be capable of receiving information via the Bluetooth link from the mobile device **100**, and also capable of sending that information via the NFC link to the universal card **110**. The short range transceiver **106** would also be capable of communicating in the opposite direction, receiving information via the NFC link from the universal card **110** and sending that information via the Bluetooth link to the mobile device **100**. One example of a two-type transceiver is a MyMax sticker produced and sold by TwinLinx of France. The MyMax sticker can be attached to the housing of a Bluetooth-enabled device, can communicate with the device via a Bluetooth connection, and can communicate via an NFC connection with an NFC-enable device.

Also depicted in FIG. **1** is a universal card **110**. The universal card **110** may include components such as a display **112**, a power source **113**, a processor **114**, and memory **115**. Each of those components are similar in function to the corresponding components of the mobile device **100**, except that the component of the universal card **110** may be physically configured differently so as to fit in the shape of the universal card **110**. For example, the display **112** of the universal card **110** may be integrated into universal card **110** via hot lamination processes and standard inlay constructs so that the universal card **110** will be the approximate shape and size of a traditional credit card and generally compliant with ISO 7810 standards.

The universal card **110** may also include a dynamic magnetic stripe **111** which can be configured to emulate the magnetic stripe of any traditional card. The standard magnetic stripe format is defined by ISO/IEC 7810:2003, and its extensions, including ISO/IEC 7811-1:2002 through ISO/IEC 7811-9:2008, and ISO/IEC 7813:2006, each of which are hereby incorporated by reference. Traditional magnetic

stripes include a series of tiny bar magnets which can be magnetized in either a north- or south-pole direction. When the polarity of the bars aligns in the same direction, the card is blank. To write data to the card, the polarity of a bar is reversed so that the north pole is facing the north pole of the adjacent bar (N-N) or the south pole is facing the south pole (S-S). This causes a change in the magnetic field that can be detected by a card reader. The two possible flux reversals, N-N or S-S, can represent two different information states, which corresponds nicely to the binary system (ones and zeros) used by computers.

Magnetic stripes have three standard track layouts: Track 1, Track 2, and Track 3. Referring to FIG. **2**, depicted is a traditional card **201** with a static magnetic stripe **202**. The static magnetic stripe includes each of Tracks 1, 2, and 3, shown as **203**, **204**, and **205**, respectively. Each of the track layouts are 0.110 inches high. Track 1 has 210 bits per inch (bpi) with room for 79 characters of 7 bits each (6 data bits, plus 1 parity bit). Track 2 has 75 bpi with room for 40 characters of 5 bits each (4 data bits, plus 1 parity bit). Track 3 has 210 bpi with room for 107 numeric digits. Tracks 1 and 2 have a standard for the data content contained in each track. Those standards are shown in Tables 1 and 2 below. In contrast, Track 3 does not have a standard for the data content in the track, and can be used for proprietary data formats.

TABLE 1

Standard Track 1 Data Content in Magnetic Stripe of Financial Cards

Data Field	Content of Data Field
Start sentinel	1 byte (the % character)
Format code	1 byte alpha ("A" is reserved for proprietary use of the card issuer; "B" is a standard for financial institutions; "C"-"M" are reserved for use by ANSI; and "N"-"Z" are available for use by individual card issuers)
Primary Account number	Up to 19 characters
Separator	1 byte (the ^ character)
Country code	3 bytes (optional)
Surname	Variable number of bytes
Surname separator	1 byte (the/character)
First name or initial	Variable number of bytes
Space	1 byte (used only when more data follows the first name or initial)
Middle name or initial	Variable number of bytes
Period	1 byte (the . character; used only when followed by a title)
Title	Variable number of bytes (optional)
Separator	1 byte (the ^ character)
Expiration date or separator	4 bytes (YYMM format), or a 1-byte separator if non-expiring card
Discretionary data	Variable number of bytes (optional; can be used by the card issuer)
End sentinel	1 byte (the ? character)
Longitudinal redundancy check	1 byte

TABLE 2

Standard Track 2 Data Content in Magnetic Stripe of Financial Cards

Data Field	Content of Data Field
Start sentinel	1 byte (the ; character)
Primary account number	Up to 19 bytes
Separator	1 byte (the = character)

TABLE 2-continued

Standard Track 2 Data Content in Magnetic Stripe of Financial Cards

Data Field	Content of Data Field
Country code	3 bytes (optional)
Expiration date or separator	4 bytes (YYMM format), or a 1-byte separator if non-expiring card
Discretionary data	Variable number of bytes (optional; can be used by the card issuer)
End sentinel	1 byte (the ? character)
Longitudinal redundancy check	1 byte

Traditional financial cards from the banking industry, such as credit cards and debit cards, typically use both Tracks 1 and 2, with Track 2 using format code "A" or "B". Some traditional credit and debit cards do not have Track 3 physically present on the cards as its data is not necessary for the cards' use. Eliminating Track 3 can reduce the physical size of the magnetic stripe. Traditional financial cards usually include all of the data listed in Tables 1 and 2.

Traditional gift cards typically use Track 2 with format code "B". Those cards usually have a unique account number, but usually do not contain the name of the user in the track. Some traditional gift cards can include the amount available at the time of the original purchase in the magnetic track, and some will store the current balance on the card so that the card can be used at any terminal. However, most traditional gift cards do not have any value data stored on the card; the card merely stores the unique account number, and each terminal at the store is connected to a database, where the value of the card is associated with the unique account number.

Traditional loyalty cards typically use Track 2 with format code "B". Like traditional gift cards, traditional loyalty cards typically include only a unique account number without storing any data about the user or any monetary value associated with the card. Most terminals which accept loyalty cards are connected to a central database which associates data about the user with the unique account number. Some traditional loyalty cards also include a barcode printed on the face of the card so that the card can be read by a barcode scanner. The barcode is representative of the unique account number of the user, and typically has no other data encoded in the barcode itself.

Many driver's licenses issued in the United States have a magnetic stripe on them. Driver's licenses typically include Tracks 1, 2, and 3. The data content of Tracks 1 and 2 are shown in Table 3. The data content of Track 3 is not entirely standardized, but Track 3 typically includes at least some of the following data categories: template number, security number, postal code, class, restrictions, endorsements, sex, height, weight, hair color, eye color, ID number, error correction, and security field.

TABLE 3

Standard Track 1 and Track 2 Data Content of US Driver's Licenses

	Content of Data Field
Track 1 Data Fields	
Start sentinel	1 character (usually the % character)
State or province	2 characters
City	Up to 13 characters (variable length)
Field separator	1 character (usually the ^ character), unless the City field is maxed out
Last name	Variable length
Field separator	1 character (usually the $ character)

TABLE 3-continued

Standard Track 1 and Track 2 Data Content of US Driver's Licenses

	Content of Data Field
First name	Variable length
Field separator	1 character (usually the $ character)
First name	Variable length
Field separator	1 character (usually the ^ character)
Home address	Variable length (usually house number and street)
Field separator	1 character (usually the ^ character)
Discretionary data	Variable length
Start sentinel	1 character (usually the ^ character)
Track 2 Data Fields	
ISO issuer ID number	6 character
License/ID number	8 character
Field separator	1 character (usually the = character)
Expiration date	4 characters (usually YYMM format)
Birth date	8 characters (usually YYYYMMDD format)
License/ID number overflow	Variable length

Traditional access cards are used to provide access to the card holder to a building or other secure area. Traditional access cards typically use either a magnetic stripe or a radio transmitter to convey information to a terminal. When using a magnetic stripe, the data encoded on the magnetic stripe typically includes the user's name, an ID number associated with the user, and an access level relating to where and when the user is allowed access. When using a radio transmitter, the access card typically only includes an ID number associated with the user, and the access terminal is connected to a database which contains information about the user and the access level based on the ID number. Radio transmitters in access cards can either be "active" radio transmitters (powered by a power source on the card), or "passive" radio transmitters (powered by the radio receiver in the terminal when the card is brought into close proximity with the terminal).

Referring back to FIG. **1**, universal card **110** can also include a radio communications apparatus **117** to emulate an access card which uses a radio communications apparatus. Radio communications apparatus **117** can either be a passive radio transmitter, or an active radio transmitter powered by power source **113**. The ID number transmitted by the radio communications apparatus **117** can be programmed so that the universal card can programmed to emulate different traditional access cards. When programming the universal card **110** to emulate an access card, it may be desirable to verify the identity of the user prior to programming the universal card **110**. Examples of user verification are discussed below.

Other types of traditional cards exist and can be emulated by universal card **110**. Examples of dynamic magnetic stripes are shown in US Patent Application Publication 2005/0194452, applied for by Nordentoft et al, and 2007/0189581, applied for by Nordentoft et al. In these examples, individually inducible transducer coils are positioned within a universal card and are configurable to emulate the static magnets in a traditional magnetic stripe. The dynamic magnetic stripe **111** of the universal card can be configured to emulate any traditional static magnetic stripe, including any data or data format used by a static magnetic stripe. Thus, even if a data content format is not discussed here, dynamic magnetic stripe **111** would be capable of emulating the data content format not discussed here.

Universal card **110** may include a biometric security device **118**, such as a fingerprint reader, a microphone for voice identification, or other device for input during biometric identification. The use of such biometric identification for security is discussed below.

Referring now to FIG. **3**, depicted is a flowchart process for programming a universal card. To initiate power on the universal card (UC) the user may be required to take an action that may include pushing a button on card to turn it "on", is tapped **301**, or any other similar technique. The universal card's power is verified **302**. If the power is not on, the user will repeat the action to initiate power **301** on the universal card again. If the power is on, the universal card and the mobile device are paired **303**, establishing the short range communication link **120** (as shown in FIG. **1**). The pairing is verified **304**, with the pairing **303** attempted again if the pairing is not successful. Once paired, an e-wallet application on the mobile device is automatically launched **305**. If the e-wallet application is not automatically launched **306**, it can be manually launched **307** on the mobile device.

Before allowing access to view, change or modify the financial data associated with the e-wallet program **105** on the mobile device **100** or on the universal card **110**, the user must first be authenticated **308**. Authentication can take a number of forms. One form of authentication can be verification of something that the user has in their possession. In this context, one security feature could be that the mobile device **100** can only be paired with one universal card **110**, and the universal card **110** will only pair to one mobile device **100**. For example, if a user's mobile device **100** is lost or stolen, the universal card **110** will not pair with any other mobile device. Thus, any personal card information stored on the universal card **110** will not be accessible by another mobile device.

Another form of user authentication can be verification of something that the user knows. This can be a personal identification number (PIN), a unique identification of the user (such as a social security number), a fact about the user (such as the maiden name of the user's mother), a password, or anything else that the user can input. Yet another form of user authentication is something about the user. This can include a fingerprint, a voice identification, or other verifiable biometric.

While each of these forms of authentication can alone authenticate the user, it may be desirable to require at least two forms of authentication to ensure increased security. For example, the mobile device **100** and the universal card **110** may authenticate each other as being paired; however, this fact alone does not ensure that the person operating the devices is the authentic user. In this case, it may be advantageous to require the user to enter a password to verify that the user is authentic. In some instances, the issuer of the card may impose additional requirement depending on the circumstances that the card is being used. For example, if the card is being used to make a payment over a certain value, if the card is being used in a foreign country, or if the card issuer has reason to suspect that the use of the card is unauthorized, the issuer may require another level of authentication. In this case, if the initial authentication included pairing authentication and a user password, the issuer may require an additional biometric authentication.

Any user input required for authentication can be entered into either the universal card **110** or the mobile device **100**. The universal card **110** may have a user interface (not shown), an optional biometric security device **118**, or other input mechanism which allows the user to input the required value. Similarly the mobile device **100** may have a user interface **104**, an optional biometric security device (not shown), or other input mechanism.

Once the user authentication **308** occurs (e.g., a password is entered), the authentication is verified **309** (the entered password is verified). If the authentication was not successful, user authentication **308** can be attempted again. If the authentication is successful, the user is prompted to select **310** an action for programming the universal card.

Notwithstanding the foregoing, it should be clear to a person skilled in the art that radio interfaces **120**, **410**, **430**, **450**, **510**, and **520** may be subject to eavesdropping or other intrusive information breaches can be protected by data encryption technologies public key, private key and other known and standard methods of radio protection.

The universal card can be programmed in many ways, including three distinct modes. First, the universal card can be programmed in a "dummy card" mode, where the universal card does not itself store any of the information required for emulation of a traditional card. In this case, the user must use the mobile device to program the universal card for each use of the card. Once the universal card is used once as programmed, it would not retain that programmed setting, and it would require re-programming if it were to be used again. Second, the universal card can be programmed in a "temporary card" mode, where the universal card stores only one set of information required for emulation. The user utilizes the mobile device to program the card to emulate a specific card either for a set amount of time or number of transactions. Once programmed in this mode, the universal card would remain programmed to emulate that one card for the set time or the number of transactions. If the user wanted to change the universal card to emulate a different card, the user would need to reconnect the mobile device to reprogram the card. Third, the universal card can be programmed in a "default card" mode, where the universal card always emulates a specific card, unless programmed otherwise. In this mode, the information of the default card is saved in the universal card and the universal card is always configured to emulate the default card, unless the user re-programs the universal card to temporarily act as another card or to change to a new default card.

It may also be possible to program the universal card in different modes for the various ways in which the universal card can be used. For example, a universal card which has both a dynamic magnetic stripe and an NFC transceiver can be used to interface with both magnetic stripe readers and NFC-equipped terminals. The user may use the universal card as a public transportation pass which makes fare payments to an NFC-equipped terminal, and as a credit card with a magnetic stripe reader. In such a case the user may program the NFC transceiver to operate in a "default card" mode, always capable of emulating the public transportation pass, but program the dynamic magnetic stripe in a "dummy card" mode where the user must program the universal card with a specific credit card to emulate before each transaction.

Once the user selects **310** an action for programming, the data required for the programming action is determined **311**. In order for the universal card to be programmed to emulate a magnetic stripe of a payment card, the universal card would need all the data required to be in the dynamic required stripe. The data could include all the information needed to fill Track 1 and Track 2, as discussed above and shown in Tables 1 and 2. The required data may be stored on the mobile device, the universal card, or a remote location such as a trusted service manager. If it is determined **312** that the required data is not available, the user is prompted to select **310** another action for programming.

If the required data is available, the universal card is programmed **314** to emulate the selected card with the required data. If the required data is stored only on the mobile device, the programming **314** will include transmitting the required data to the universal card via the short range communication link. If the required data is stored on the universal card, the programming **314** need only include configuring the appropriate device (e.g., dynamic magnetic stripe, short range transceiver, radio transmitter, etc) properly for emulation.

Referring to FIG. **4**, depicted are interactions between the mobile device **100** and the universal card **110**, and between the universal card **110** and three different types of terminals **400**, **420**, and **440**. As discussed above, the mobile device **100** communicates with the universal card **110** via a short range communications link **120** to program the universal card **110** for emulation of traditional cards. The universal card **110**, in turn, can communicate with terminals **400**, **420**, and **440** in a number of ways. It is important to note that, once universal card **110** is programmed, the short range communications link **120** between the mobile device **100** and the universal card **110** need not be established for the universal card **110** to interact with the terminals **400**, **420**, and **440**.

Terminal **400** is equipped with a magnetic stripe reader **401** which can read the dynamic magnetic stripe **111** of the universal card **110** when it is swiped **410** through the magnetic stripe reader **401**. The magnetic stripe reader **401** can read any of the data written to the dynamic magnetic stripe **111**. Terminal **420** is equipped with a short range transceiver **421** which can establish a short range communication link **430** between the universal card **110** and the terminal **420**. Any required data can be transmitted from the universal card **110** to the terminal **420** via the short range communication link **430**. Terminal **440** is equipped with a radio receiver **241** which can receive data sent from the radio transmitter **117** of the universal card **110**. Any required data can be transmitted from the universal card **110** to the terminal **440** via the radio link **450**.

One potential problem with the e-wallet software **105** on the mobile device **100** is that large amounts of information may need to be inputted into the e-wallet software **105**. The user interface **104** may not be convenient for entry of the large amounts of information. Also, management of the information in the e-wallet software **105** may also not be convenient via the user interface **104**. To address this issue, a personal computer **500** can be used.

Referring to FIG. **5**, depicted is an exemplary system including the personal computer **500**, the mobile device **100**, and the universal card **110**. The personal computer can include a processor **501**, memory **502**, a power source **503**, a user interface **504**, the e-wallet software **505**, and a communications port **506**. The processor **501**, memory **502**, power source **503**, and user interface **504** are all similar in function to the corresponding components of the mobile device **100**, as discussed above. The e-wallet software **505** can be the same or similar to e-wallet software **105** of the mobile device **110**. The user may enter data and manage the card data in e-wallet software **505** in the same way the user would use e-wallet software **105**.

When the user enters data or makes changes in the management of e-wallet software **505**, the e-wallet software **105** on the mobile device **100** must be updated to reflect the new and/or changed data. In order to make these updates, a communication link **510** can be established between the communication port **506** of the personal computer **500** and the communication port **107** of the mobile device **100**. The communication link **510** can be any type of wired or wireless link, including a serial cable, a wired or wireless local area network (LAN), a wired or wireless wide area network (WAN), a short range communication link, a radio link, or any similar connection. Alternatively, a communication link **520**

can be established between a short range transceiver **507** of the personal computer **500** and the short range transceiver **106** of the mobile device **100**.

Once a communication link is established between the personal computer **500** and the mobile device **100**, the data in e-wallet software **505** and the e-wallet software **105** can be synchronized. It is important to note that the short range communication link **120** between the universal card **110** and the mobile device **100** need not be active for the link **510** or the link **520** to be established between the personal computer **500** and the mobile device **100**.

Referring to FIG. **6**, depicted is a flowchart process for managing universal card data using mobile device **100**. The e-wallet software is launched **601** on the mobile device. Before the user is given access to the e-wallet software, the user must first login and be authenticated **602**. Authentication here can be the same or similar to the forms of authentication discussed above. A determination is made whether the authentication is successful **603**. If not successful, the user is prompted to login and authenticate **602** again. If the authentication is successful, the user is allowed to control **604** the e-wallet software a user interface of the mobile device.

The control **604** of the e-wallet software includes anything that the user may need to do to prepare for programming the universal card or to program the universal card. The user can enter data associated with a traditional card or with a financial account. The user can manage the entered data such as by naming a particular account or traditional card, setting a default card, or any other management action needed.

After the user enters data, the data is verified **605**. The verification can include determining whether sufficient data has been entered for emulation of a traditional card, or whether the data entered matches the data of the card issuer. If the data is not verified, the user is allowed to reenter data **604**. If the data is verified, the data is encrypted **606** for storage. Encrypting the data for storage is another form of security, as someone that gains access to the encrypted data cannot recover the entered data without knowing how to decrypt the encrypted data. After the data is encrypted, the encrypted data can be stored **607** to the mobile device.

A determination **608** is made as to whether the encrypted data should be uploaded to the personal computer. If the encrypted data will not be uploaded, no further action is required. If the encrypted data will be uploaded to the personal computer, the communication connection between the mobile device and the personal computer is either established or checked **609**. If the connection to the computer is not verified **610**, another attempt to establish **609** the connection can be attempted. Once the connection to the computer is verified **610**, the encrypted data can be uploaded and saved **611** to the personal computer.

Referring to FIG. **7**, depicted is a flowchart process for managing universal card data using personal computer **500**. Many of the steps are similar to those depicted in FIG. **6**. The PC version of the e-wallet software is launched **701**. The user goes through login and authentication **702** which is verified **703**. Once the user authentication is verified, the user can control **704** the e-wallet software via a user interface of the personal computer. The control on the personal computer is the same as the control on the mobile device, except that the user may prefer to use the user interface of the personal computer to the user interface of the mobile device.

Data entered on the personal computer can be verified **705**. Once verified, the data is encrypted **706** for storage. The encrypted data is stored **707** on the personal computer. A determination **708** is made as to whether the encrypted data should be uploaded to the mobile. If the encrypted data will not be uploaded to the mobile device, the no further action is required. If the encrypted data will be uploaded, the communication connection between the mobile device and the personal computer is either established or checked **709**. If the connection to the computer is not verified **710**, another attempt to establish **709** the connection can be attempted. Once the connection to the computer is verified **710**, the encrypted data can be uploaded and saved **711** to the mobile device.

The visible sides of a universal card may be designed in a number of ways to provide a user with access to information or components of the universal card. FIG. **8**A depicts one design of the front of a universal card **800**. The front of the universal card **800** can have a brand area **801** which can be used to identify the brand of the universal card issuer, the brand of a wireless carrier, the brand of a sponsor, any other brand, or any combination of those brands. The front of the universal card **800** can have the name of the card holder **802** on the face of the card to identify the user. The front of the universal card **800** can also have a display **803** which could be used at various times to display an account number, an expiration date, a card issuer logo, any other information, or any combination of these types of information. The front of the universal card **800** could also include a biometric security reader **804**, such as a fingerprint reader, which is used to authenticate the user.

FIGS. **8**B, **8**C, and **8**D depict other possible designs for the front of a universal card. FIG. **8**B depicts the front of a universal card **810** which is similar to the front of universal card **800**, including a brand area **811**, the name of the card holder **812**, a display **813**, and a biometric security reader **814**. The front of the front of the universal card **810** can also have an EMV chip **815** which is a required component of cards in some markets including some European markets. FIG. **8**C depicts the front of a universal card **820** which is similar to the front of universal card **800**, including a brand area **821**, the name of the card holder **822**, and a biometric security reader **824**; however, the front of universal card **820** does not include a display. FIG. **8**B depicts the front of a universal card **830** which similar to the front of universal card **800**, including a brand area **831**, the name of the card holder **832**, a display **833**, and a biometric security reader **834**. The front of universal card **830** also shows that the name of the card holder **832** and the display **833** can be located in various locations on the front of a universal card.

FIG. **9** depicts one design of the back of a universal card **900**. The back of universal card **900** can include a dynamic magnetic stripe **901** for interacting with a terminal, a signature area **902** which displays the signature of the card holder, and a brand area **903**. Similar to the brand area **801** described above, brand area **903** can be used to identify the brand of the universal card issuer, the brand of a wireless carrier, the brand of a sponsor, any other brand, or any combination of those brands.

FIGS. **10**A and **10**B depict an embodiment of a universal integrated circuit card. In general, an integrated circuit card (also sometimes referred to as a "contact card," an "IC card," a "chip and PIN card," an "EMV card," and so forth) is a card that has an embedded integrated circuit and can be authenticated automatically using a PIN. To reduce fraud, banks and retailers are replacing traditional magnetic stripe equipment with integrated circuit cards. When a customer wishes to pay for goods using this system, the card is placed into a "PIN pad" terminal or a modified swipe-card reader, which accesses the chip on the card. Once the card has been verified as authentic, the customer enters a PIN, which is submitted to the chip on the integrated circuit cards. The chip verifies

whether the PIN is correct and replies accordingly to the terminal. Integrated circuit cards have been effective to significantly cut card-present (face-to-face) fraud.

The EMV standard is one standard that has been developed for integrated circuit cards; the EMV standard defines the physical, electrical, data, and application interactions between an integrated circuit card and the terminal. As mentioned above, an EMV chip is a required component of cards in some markets including some European markets. Other forms of integrated circuit cards, such as the Chip and PIN system, are used in other markets.

Increasingly it is becoming important for US citizens to have a card with both a magnetic stripe and an integrated circuit, so that when a person is traveling internationally it is easier for them to pay with a US credit card. In many countries, merchants reject credit cards with only a magnetic stripe. Thus, in order for a universal card to be usable worldwide, it must also include an integrated circuit. One difficulty with including an embedded integrated circuit with a universal card is that the integrated circuit can be associated only with a single credit or debit card.

EMV cards use a cryptographic engine which authenticates the card, the transaction, and the card holder each time that the card is used in a transaction. By authenticating the card, the transaction, and the card holder, EMV card transactions are more secure than magnetic stripe card transactions were the card data on the magnetic stripe can be skimmed and cloned for use in fraudulent transactions.

EMV cards can be authenticated in both online transactions and offline transactions. An online transaction is a transaction in which the terminal is connected to a card authorization service, such as a card authorization service provided by a card issuer. An offline transaction is a transaction in which the terminal is not connected to a card authorization service. In an online transaction, the EMV card is authenticated using dynamic data authentication (DDA). During a DDA session, the EMV card creates a unique digital signature for the particular transaction. The digital signature is based on a public key that is stored in the EMV card and signed by a certification authority. A random number for the particular transaction is generated by the terminal and the digital signature is changed based on the random number. The digital signature is then verified by the card authorization service using the public key. In an offline transaction, the card is authenticated by the terminal using static data authentication (SDA), DDA, or a cryptogram generation authentication (CDA) and DDA. SDA is an asymmetric digital signature scheme that uses public and private keys to encode and decode the data. The private key is only known by the card issuer, whereas the public key is known by every terminal CDA is a dynamic signature similar to DDA where the signature is generated in the EMV card and verified by the terminal.

Transactions using EMV cards can be authenticated during transactions. Card issuers typically define the rules for authenticating transactions with their EMV cards. In an online transaction, transaction information, which similar to card data on a static magnetic stripe, along with a transaction specific cryptogram are sent to an authorization service for transaction authorization. In an offline transaction, the terminal and EMV card exchange card information and the terminal can approve or reject the transaction.

Cardholders of EMV cards can be authenticated during transactions. Card issuers typically define the rules for authenticating transactions with their EMV cards. During a transaction, a cardholder can enter a PIN into the terminal. In an online transaction, the PIN can be verified by an authorization service or at the terminal. In an offline transaction, the PIN can be verified by the terminal. Alternatively, the cardholder can sign a receipt and the signature can be compared to a signature on the EMV card.

The level of verification that a terminal may require can depend on the amount of risk associated with the transaction. In some cases, such as in offline transactions, the terminal may limit an amount for any given transaction to protect against fraud and credit overruns.

Referring back to FIGS. **10**A and **10**B depict an embodiment of a universal integrated circuit card **1000**. The universal integrated circuit card **1000** has a front **1010** that can include an EMV chip **1011**. The front of the card **1010** can also include features such as the card holder's name **1012**, a display **1013**, and a brand area **1014**. The universal integrated circuit card **1000** also has a back **1020** that can include a dynamic magnetic stripe **1021**. The back of the card **1020** can also include features such as a signature area **1022** and a brand area **1023**. The universal integrated circuit card **1000** can include any or all of the features described above with respect to universal card **110**. Thus, the universal integrated circuit card **1000** can communicate with a mobile device be programmed to emulate traditional magnetic stripe cards using the dynamic magnetic stripe **1021**, and the universal integrated circuit card **1000** can interact with point-of-sale terminals that include magnetic stripe readers, short range transceivers, radio communication apparatuses, and the like. In addition, the EMV chip **1011** of universal integrated circuit card **1000** can be associated with a default credit or debit card. In this configuration, the universal integrated circuit card **1000** can be used with the default credit or debit card associated with the EMV chip **1011** at any terminal that requires an EMV chip and the universal integrated circuit card **1000** can be used to emulate any other card using the dynamic magnetic stripe **1021**, a short range transceiver (not shown), a radio communication apparatus (not shown), or similar communication mechanism.

When a user orders or otherwise obtains a universal card **1000**, the user can select or order a universal card **1000** that has an EMV chip **1011** associated with a particular default credit or debit card. The default credit or debit card associated with the EMV chip **1011** can be the same or different from a default card associated with the dynamic magnetic stripe **1021**. For example, the user may have a VISA credit card that is the default card for the dynamic magnetic stripe **1021** and the same VISA credit card may be the default card associated with the EMV chip **1011**. In this example, the user is accessing the same VISA credit card whether the transaction uses the EMV chip **1011** or whether the transaction uses the default card associated with the dynamic magnetic stripe **1021**. In another example, the user may have a DISCOVER credit card that is the default card for the dynamic magnetic stripe **1021** and the user may have a MASTERCARD credit card that may be the default card associated with the EMV chip **1011**. This example may be ideal for a user who lives in the United States and frequently wants to use the DISCOVER credit card for purchases at magnetic swipe terminals in the United States, but also frequently travels to Europe and wants to use the MASTERCARD credit card for purchases at EMV terminals in Europe. In either example, while the EMV chip may not be dynamically programmable, the universal integrated circuit card **1000** would still be programmable to emulate other cards, such as an AMERICAN EXPRESS credit card, using the dynamic magnetic stripe **1021**, a short range transceiver, or a radio communication apparatus.

Referring now to FIGS. **11**A and **11**B, depicted is another embodiment of a universal card **1100**. The universal card **1100** has a front **1110** that can optionally include a card

holder's name **1111**, a display **1112**, and a brand area **1113**. The universal card **1100** also has a back **1120** that can include a dynamic magnetic stripe **1121**. The back of the card **1120** can also include features such as a signature area **1122** and a brand area **1123**. The universal integrated circuit card **1100** can also include a secure element **1130**, which can be located on the front, the back, or in the interior of universal integrated circuit card **1100**.

A secure element **1130** is a tamper-proof smart card chip capable of embedding smart card grade applications, such as bank cards, credit cards, transportation cards, and the like, with the level of security required by financial institutions. Secure elements have been included in some computing devices, such as smart phones, as an independent part of the computing system which stores data associated with traditional cards and runs any software applications that use the traditional card data. Card issuers typically require this independent secure element to be in the computing device to ensure the security of the traditional card data and to protect against fraud. This requirement puts a limitation on developers and distributors of software application that use traditional card data because the ability to use such software applications is limited to computing devices which have secure elements. For example, a software developer may create a software application that runs in a cell phone operating system, such as the ANDROID operating system. The ANDROID operating system is available for use on a wide variety of cell phone models, only a few of which have secure element hardware. Thus, the software application will be limited to use on only those cell phone models that have a secure element and cannot be used on ANDROID cell phones that do not have a secure element.

In the embodiment depicted in FIGS. **11**A and **11**B, the universal card **1100** includes a secure element **1130** in the card. The universal card **1100** can communicate with any computing device, regardless of whether the computing device has a secure element. In the case where the universal card is in communication with a cell phone that does not have a secure element, the universal card **1100** can make secure element **1130** available for use by the cell phone. Thus, a user will be able to use software applications on the cell phone that require a secure element by utilizing the secure element **1130** of the universal card **1100** while the cell phone is in communication with the universal card **1100**. Furthermore, the user can enter traditional card information into the cell phone while the cell phone is in communication with the universal card **1100**, the traditional card data can be communicated to the secure element **1130** of the universal card **1100** for storage, and the cell phone can later access the traditional card data in the secure element **1130** of the universal card **1100** in the same or a later communication session. Including a secure element **1130** in universal card **1100** solves the issues associated with computing devices that do not have a secure element. In addition, including a secure element **1130** in universal card **1100** allows banks and card issuers to have greater control of the use of secure elements. Currently, when mobile device manufacturers include secure elements in mobile devices, banks and card issuers must negotiate with the manufacturers to be able to have access to and use of the secure element. However, moving the secure element to a universal card **1100** which is under control of the bank or card issuer eliminates the need for the bank to negotiate with the manufacturer of a mobile device to have access to a secure element regardless of whether the mobile device also has a secure element.

Referring now to FIGS. **12**A and **12**B, depicted is another embodiment of a universal card **1200** having a secure element and an EMV chip. The universal card **1200** has a front **1210** that can optionally include a card holder's name **1211**, a display **1212**, and EMV chip **1213**, and a brand area **1214**. The universal card **1200** also has a back **1220** that can include a dynamic magnetic stripe **1221**. The back of the card **1220** can also include features such as a signature area **1222** and a brand area **1223**. The universal integrated circuit card **1200** can also include a secure element **1230**.

Referring now to FIG. **13**, depicted is an embodiment of a universal card **1300** with a power indicator **1310**. The power indicator **1310** indicates to the user that the universal card **1300** is ready to be used in a transaction. The power indicator **1310** can indicate that the universal card **1300** can be used with either or both of a magnetic stripe reader and a contactless payment terminal. The power indicator **1310** can be any visual indicator, such as an LED light, a color indicator, and the like. In the embodiment of an LED light, the LED light can be illuminated when the card is active (i.e., ready to emulate a traditional card as either or both of a magnetic swipe card or a contactless payment card) and the LED light can be off when the card is inactive. A power indicator **1310** on universal card **1300** can replace the need for the universal card **1310** to have a display, thereby reducing the overall cost to make and sell the universal card **1310**. As depicted in FIG. **13**, the power indicator **1310** can be located on a front **1320** of universal card **1300**. Optionally, the front **1320** of universal card **1300** can also include the card holder's name **1321** and a brand area **1322**. In another embodiment not depicted in FIG. **13**, a power indicator can be located on a back of universal card **1300**.

One benefit associated with the use of a power indicator **1310** is that a card holder will know that the card is active when attempting to use the card. As discussed above, a universal card can be programmed to emulate a default card unless programmed otherwise by the card holder. In this situation, the card holder may assume that the universal card can be used at any moment as the default card. However, the universal card may be programmed to be inactive when not in use in order to conserve battery power. If the universal card is inactive and there is no power indicator, the card holder may assume that an inactive card is always active and attempt to use the inactive universal card as the default card. Having a power indicator **1310** on the universal card **1300** allows the user to easily determine whether the universal card **1300** is active and ready for use.

Referring now to FIG. **14**, depicted is an embodiment of a universal card **1400** with a switch **1410**. The switch **1410** enables the user to activate or deactivate the universal card **1400**. Having a switch **1410** on the universal card **1400** eliminates the need for the user to interact with a mobile device in communication with the universal card **1400** to activate the universal card **1400**. For example, the universal card **1400** may be programmed to emulate a default card unless programmed otherwise by the card holder. If the card holder simply wants to use the universal card **1400** to emulate the default card, the card holder can activate the universal card **1400** using the switch **1410** and not have to use a mobile device in communication with the universal card **1400** to activate the universal card **1400**. The switch can be especially useful if the user's mobile device is out of battery power or otherwise malfunctioning. When the universal card **1400** is activated using the switch **1410**, the universal card **1400** can retrieve the information for the default card from a secure element in universal card **1400**. Thus, no exchange of information between a mobile device and universal card **1400** is necessary to activate universal card **1400** to be the default card using the switch **1410**.

A bank or card issuer of a universal card may take advantage of the default card feature of the universal card. The bank or card issuer may require the consumer to download and use its e-wallet software application to interface with the universal card. That e-wallet software may require that the default card of the universal card is a default card which is issued by the bank or card issuer. For example, if a bank issues the universal card and requires the consumer to download the bank's e-wallet software, the bank's e-wallet software may allow the consumer to select only one of the bank's cards, such as a debit card associated with the bank or a credit card associated with the bank, as the default card. In this scenario, each of the default cards associated with the universal card, including a default card for an EMV chip, a default card for a dynamic magnetic stripe, and a default card for contactless payment, may be a card associated with the bank. Arranging for all of the default cards to be associated with the bank is a valuable position for the bank because the easiest way for the consumer to use the universal card is by using the universal card as one of the default cards without using a mobile device to change the universal card to a non-default card.

The switch **1410** can take any number of forms. As depicted in FIG. **14**, the switch **1410** could be a button on the exterior of universal card **1400**, such as on a front **1420** of universal card **1400**. Optionally, the front **1420** of universal card **1400** can also include the card holder's name **1421** and a brand area **1422**. In another embodiment not depicted in FIG. **14**, a switch can be located on a back of universal card **1400**. In addition, the universal card **1400** could include both a switch **1410** and a power indicator (not shown in FIG. **14**). This combination would allow the card holder to activate the universal card **1400** using the switch **1410** and visually see that the universal card **1400** has been activated. In another form of the switch not depicted in FIG. **14**, the switch **1410** could be snap switch on the interior of the card. A snap switch can detect bending and/or tapping of the universal card **1400**. Using a snap switch, in order for the card holder to activate the card, the card holder would slightly bend and/or tap the card until the universal card is active. In the embodiment of a snap switch, a power indicator on the card may be particularly helpful so that the card hold knows when the card has been sufficiently bent and/or tapped to trigger the snap switch.

Referring now to FIGS. **15**A and **15**B, depicted are ways to add traditional card data to a secure element of a universal card. As shown in FIG. **15**A, a card holder can have one or more traditional cards **1510**. The user can swipe the one or more traditional cards **1510** through a magnetic stripe reader **1520** which reads the traditional card data from the swiped magnetic stripe. The magnetic stripe reader **1520** is connected to a mobile device **1530** which is configured to receive the traditional card data from the magnetic stripe reader **1520**. The connection between the magnetic stripe reader **1520** and the mobile device **1530** may be a wired connection or wireless connection. The mobile device **1530** can be connected to a universal card **1540** which has a secure element **1541** via a short range communication link. The mobile device **1530** is configured to transmit the traditional card data received from the magnetic stripe reader **1520** to the universal card **1540** without storing the traditional card data, and the universal card **1540** is configured to store the traditional card data in the secure element **1541**. In one embodiment of the connection between the magnetic stripe reader **1520** and the mobile device **1530**, the magnetic stripe reader **1520** has a headphone connector which is configured to connect to a headphone port of the mobile device **1530**, and the mobile device **1530** is configured to receive the traditional card data from the magnetic stripe reader **1520** via the headphone port.

As shown in FIG. **15**B, a computing device **1550** can store traditional card data in storage **1551**. The computing device **1550** can also have a processor **1552** and other computing hardware and/or software. The computing device **1550** can be controlled and secured by a bank, by a traditional card issuer, or by another entity. The computing device **1550** is connected to a mobile device **1570** via a network **1560**. The network **1560** can be a wired network, a wireless network, or any combination of wired and wireless networks, including one or more of the internet, a cellular phone network, a wi-fi network, a local area network, a wide area network, and the like. The mobile device **1570** is configured to receive the traditional card data from the computing device **1550** via the network **1560**. The computing device may encrypt the traditional card data prior to transmission via the network **1560**. The mobile device **1570** can be connected to a universal card **1580** which has a secure element **1581** via a short range communication link. The mobile device **1570** is configured to transmit the traditional card data received from the computing device **1550** to the universal card **1580** without storing the traditional card data, and the universal card **1580** is configured to store the traditional card data in the secure element **1581**.

Another way that a secure element of a universal card can be loaded with traditional card data is by the card issuer pre-loading the traditional card data on the secure element before the card is given to the consumer. The card issuer may have information about some or all of the consumer's traditional cards and can pre-load the secure element of a card with the traditional card data. In one example, the card issuer may be a bank and the consumer may have a debit card associated with the bank and a credit card associated with the bank. The bank may pre-load into the secure element of a universal card traditional card data corresponding to each of the debit card and the credit card before sending the universal card to the consumer. When the consumer receives the card, the universal card will already be configurable to emulate the debit card and the credit card. In one embodiment, the bank may also designate one of the debit card and the credit card as the default card for the universal card before sending the universal card to the consumer. In this embodiment, the universal card may be immediately available to the consumer for use as the default card without having to interface the universal card with a mobile device. Setting the default card to a traditional card associated with the bank gives the bank the valued position of having its traditional card be the easiest way for the consumer to use the universal card.

Referring now to FIG. **15**C, depicted is a way to use a universal card with a mobile device that includes a secure element. Traditional card data **1590** can be communicated to a mobile device **1591**. The traditional card data **1590** can be communicated by swiping traditional card through a magnetic stripe reader which communicates the traditional card data to mobile device **1591**, similar to the depiction in FIG. **15**A, or traditional card data **1590** can be communicated from a computing device to mobile device **1591** via a network, similar to the depiction in FIG. **15**B. Mobile device **1591** can include a secure element **1592** which is configured to securely and independently store the traditional card data. The mobile device **1591** can be configured to send instructions to a universal card **1593** to program the universal card **1593** to emulate a traditional card. The instructions sent from the mobile device **1591** to the universal card **1593** can include confidential traditional card data from the secure element **1592** which is necessary for the universal card **1593** to emulate the traditional card. The instructions sent from the mobile device **1591** to the universal card **1593** can include instructions for the

universal card to emulate either or both of a magnetic stripe of the traditional card and a contactless payment form of the traditional card.

Referring back to FIG. **1**, a mobile device **100** can be configured to communicate with a universal card **110** that has a secure element **119** via a short range communication link **120**. As described above, a secure element **119** is an independent part of the universal card **110** which stores data associated with traditional cards and maintains that traditional card data securely. The mobile device **100** can include e-wallet software **105** that provides a user interface which allows a user to program the universal card **110**. In one embodiment, the secure element **119** of the universal card **110** stores confidential traditional card data associated with a VISA credit card and a DISCOVER credit card. The confidential traditional card data in the secure element **119** can include any information necessary to emulate the VISA credit card and the DISCOVER credit card, such as an account number, a card number, a card holder's name, an expiration date, a card verification value 2 (CVV2), information stored on the magnetic stripe of the traditional cards, and any other required information. The e-wallet software **105** may not store the confidential traditional card data because banking requirements may not permit the confidential traditional card data to be stored on the mobile device **100**. However, the mobile device **100** may store non-confidential data for each of the traditional cards. For example, the mobile device **100** may store a nickname associated with each traditional card, the last 4 digits of the traditional card number, an image associated with the issuer of each traditional card, and so forth. By storing non-confidential traditional card data in mobile device **100**, the e-wallet software **105** can permit the user to select which traditional card the universal card **110** shown emulate by displaying some or all of the non-confidential traditional card data. For example, the e-wallet software **105** may display two buttons respectively labeled as "VISA **** **** **** 1234" and "DISCOVER **** **** **** 9876." The user can select either of the two traditional credit card options. In response, the mobile device **100** sends a signal to universal card **110** indicating that the universal card should emulate the selected traditional credit card. In one embodiment, the universal card **110** configures both the dynamic magnetic stripe **111** to emulate the magnetic stripe of the selected traditional credit card and the short range transceiver **116** to emulate the selected traditional credit with a contactless payment terminal. In this manner, the user needs only to select the desired traditional card using the e-wallet software **105**, without having to make a selection of magnetic stripe or contactless payment, and the user can use the traditional card with either a magnetic swipe terminal or a contactless payment terminal.

When the universal card **110** is in communication with the mobile device **110**, the universal card **110** may send notifications back to mobile device **100**. For example, if a battery in universal card **110** is low, the universal card **110** can send a low battery signal to the mobile device **100**. The mobile device **100** or the e-wallet software **105** can be configured to display a warning message to the user. The mobile device **100** or the e-wallet software **105** can also be configured to communicate to the issuer of the universal card **110** that the universal card **110** needs to be replaced. In another example of a notification, a VISA card may have been selected as a default card for the universal card **110**, but the user may have programmed the universal card **110** to emulate a DISCOVER card for a three-hour period and then revert back to the default VISA card. This situation may occur when the user is planning to spend several hours at a shopping mall and wants to use the DISCOVER card while at the mall. At or near the end of the three-hour period, the universal card **110** may send a signal to the mobile device that the universal card **110** is about to revert back to the default VISA card. The mobile device **100** or the e-wallet software **105** can be configured to display a warning message or sound and alarm to the user so that the user is aware of the reversion back to the VISA card.

One issue with using a mobile device **100** to interface with a universal card **110**, and any confidential data stored in a secured element of the universal card, is the need for authentication. Several forms of authentication are discussed above. Authentication may also vary based on the configuration of the mobile device **100**. For example, a mobile device **100** may be secured such that a user of the mobile device must be authenticated each time the user unlocks the mobile device **100**. In this case, the e-wallet software **105** may recognize that the user has already been authenticated when the mobile device **100** was unlocked, and the e-wallet software **105** may not need to require authentication when the user initially interfaces with the e-wallet software **105**. In another example, a user may be able to unlock the mobile device **100** without any authentication. In this case, any person may be able to unlock the device and start the e-wallet software **105**. Here, the e-wallet software **105** may recognize that the user has not been authenticated when the mobile device **100** was unlocked, and the e-wallet software **105** may require the user to be authenticated when the user initially interfaces with the e-wallet software **105**.

The issuer of the universal card **110** may have interest in making the universal card **110** available for interacting with e-wallet software created by other individuals or entities. In order to allow such third-party software to be created, the issuer may create an application programming interface (API) or software developer kit (SDK) which provides a framework of rules and specifications for interacting with the universal card **110**. The API or SDK can be provided to third party software developers to enable them to create e-wallet software applications that successfully interact with the universal card **110**.

The dynamic magnetic stripe **111** of universal card **110** may be used in a number of ways that are not available to static magnetic stripe cards. As discussed above, magnetic stripe cards have three standard track layouts: Track 1, Track 2, and Track 3. Various implementations of magnetic stripes have standard fields in certain tracks while leaving other portions of tracks available for other uses. Having a dynamic magnetic stripe **111** in a universal card **110** allows the non-standardized portions of the tracks to communicate data to a terminal that cannot be communicated by a static magnetic stripe of a traditional card. In one embodiment, a card holder may want to pay with a credit card and use one or more coupons in the same transaction. In a traditional setting, the card holder would present physical coupons to a cashier, the cashier would enter the coupons, and the card holder's traditional card would be swiped for payment. In contrast, an e-wallet application **105** can manage digital coupons for a user. Using the mobile device **100** and e-wallet application **105**, the user can select one or more coupons to be used in a transaction, and a corresponding signal can be communicated to the universal card **110**. The signal can also include an indication of a traditional card for the universal card **110** to emulate. When universal card **110** configures the dynamic stripe **111** to emulate a traditional card magnetic stripe, the universal card **110** can also include the coupon information in one of the non-standardized portions of the tracks. The universal card **110** can be swiped in a magnetic stripe reader which is configured to identify the data in the non-standard-

ized portions of the tracks. The magnetic stripe reader may apply the coupon to the transaction prior to charging the transaction to the account associated with the traditional card emulated by the universal card **110**.

Another example of using the non-standardized portions of the tracks includes using a dynamic authentication value to authenticate the transaction. To prevent fraudulent transactions, traditional contactless cards can generate dynamic data every time they are read. Dynamic data generation per read provides logical security and inhibits fraudulent replay of contactless card data that may have been previously read. For example, contactless credit, debit and prepaid payment card data includes a dynamic card verification number, sometimes referred to "CVC," "CVV," or "dynamic CVV," or transaction certificate (for EMV cards). The dynamic authentication value is unique for every transaction. One way of the dynamic authentication value to be generated is using a secret key stored in secured memory of the card, a random number, a transaction counter, and a specific algorithm. Other ways of generating the dynamic authentication value are possible. The dynamic authentication value is generated dynamically every time a traditional contactless card is read for a transaction and the dynamic authentication value can be authenticated by a payment terminal contacting the issuer of the card to verify the dynamic authentication value. However, dynamic authentication values cannot be used with traditional static magnetic stripe cards because the static magnetic stripe cannot produce a unique dynamic authentication value each time the magnetic stripe is swiped for a transaction. The use of a dynamic magnetic stripe **111** in universal card **110** allows a dynamic authentication value unique to each transaction to be written to the non-standardized portions of the tracks. In this manner, a universal card **110** can generate a dynamic authentication value in the same manner as traditional contactless cards and write the generated dynamic authentication value to one of the non-standardized portions of the tracks. The universal card **110** can be swiped in a magnetic stripe reader which is configured to identify the dynamic authentication value in the non-standardized portions of the tracks and authenticate the transaction with the card issuer. In another embodiment, the traditional card may have a field on the static magnetic stripe for a CVV value. When the universal card is configured to emulate the traditional card that normally has a static CVV value field, the universal card may generate a dynamic authentication value and write the dynamic authentication value in the field typically used for the static CVV value. The dynamic authentication value could have the same format as the static CVV and be located in the same location that the static CVV field would be located in the static magnetic stripe of the traditional card. In this scenario, there would be no need to reconfigure the terminal with the magnetic stripe reader because it would already be configured to read a value from the static CVV field location. Using dynamic authentication values with traditional magnetic stripe reader terminals allows for the added security of the dynamic authentication value authentication without requiring terminals to add a contactless payment terminal to the magnetic stripe reader.

When the universal card can be configured to emulate multiple traditional cards, some of issuers of the traditional cards will be capable of authenticating a dynamic authentication value while others of the issuers of the traditional cards will only be capable of authenticating a static authentication value. The secure element may store with the traditional card data, an indication as to whether a static authentication value or a dynamic authentication value should be used when emulating each traditional card.

A universal card can also be used to eliminate the need for physical traditional cards altogether. Traditional cards are currently being used as pre-paid cards in place of cash in a number of settings. Many credit issuing companies, such as VISA, MASTERCARD, and AMERICAN EXPRESS, offer pre-paid debit cards which require that the amount of the debit card be pre-paid, or "loaded," before the card can be used in a financial transaction. Some pre-paid debit cards permit users to pay up the available amount on the card, or "reload" the card. These pre-paid debit cards can be used by consumers who have bad credit but still want the ease of using a magnetic swipe card in transactions, by government agencies to provide government benefits such as social security benefits and unemployment benefits, by employers as bonuses or incentives to employees, and by consumers that give them as gifts. Traditional cards are also being used as gift cards which are typically usable only at a single retailer or group of retailers. Gift cards typically must be pre-paid. Consumers that buy gift cards must either go to a retail location to buy the physical gift card or they can purchase gift cards online and have the physical gift card shipped. Some retail locations, such as grocery stores, offer for purchase gift cards to a wide variety of other retail locations. This offers a consumer the convenience of purchasing gift cards for a number of different retailers while only physically visiting a single store to obtain the physical gift cards. Traditional cards are also being used as loyalty cards and membership cards for certain retail locations. Many retailers, such as grocery stores, allow consumers to obtain free loyalty cards which can be presented when the consumer is checking out to obtain sale prices of certain items. Other retailers, such as warehouse stores, offer paid memberships which include a membership card that must be presented each time the consumer is entering the store and/or checking out.

The proliferation of uses for traditional cards has flooded consumers with the number of traditional cards they may need to carry. For example, a consumer may carry several credit cards, a debit card, several gift cards, a membership card, and several loyalty cards. Having to carry so many cards may reduce the likelihood that a consumer would sign up for an additional card. For example, if a consumer is at a store that offers a loyalty card, the consumer may decline the loyalty card because the consumer does not want to carry around an additional card, to remember where that card is stored in a purse or wallet during a subsequent visit to the store, and the like. Additionally, having a large number of cards increases the likelihood that a card will be misplaced, lost, or stolen. A consumer is much less likely to purchase a pre-paid card, such as a pre-paid debit card, a gift card, and the like, if the entire value of the card is lost when the card is lost, misplaced, or stolen.

Attempts have been made to eliminate the need for physical traditional cards. Services have been developed which allow consumers to make online purchases of digital gift certificates. The digital gift certificate is typically sent to the recipient in a printable form. The recipient must print out the gift certificate and take the physical printout to the retail location to use the gift certificate. The printed gift certificate typically includes a bar code or other code which the retail location can verify before accepting the printed gift certificate as payment. While this system eliminates a physical card, it still requires the consumer to carry a printout to the retail location. Additionally, loss or theft of the printout can result is loss of the value of the gift certificate if the lost or stolen printout is used by another person.

Referring now to FIG. **16**, depicted is an electronic card data delivery system **1600**. Computing device **1610** can be

associated with an operator which distributes pre-paid cards, loyalty cards, or any other type of card. The computing device **1610** is connected, via a network **1620**, to a computing device **1630**. Computing device **1630** is associated with a universal card **1640**. A user can contact the operator of computing device **1610** and request that card data be sent to computing device **1630** for use by universal card **1640**. For example, the user can request that a $100 gift card be sent to computing device **1630**. In response to receiving the request, computing device **1610** can create a gift card account credited with $100 and deliver, via network **1620**, card data to computing device **1630**. The gift card data can be used to program universal card **1640** to emulate a traditional card associated with the gift card account. In another example, the user can request a loyalty card account and computing device **1610** can deliver, via network **1620**, card data to computing device **1630**. The loyalty card data can be used to program universal card **1640** to emulate a traditional card associated with the loyalty card account.

Electronic delivery of card data from computing device **1610** to computing device **1630** can take a number of forms. In one example, the user requesting delivery of the card data may identify computing device **1630** and the computing device **1610** may automatically send the card data to computing device **1630**. In another example, when requesting delivery of the card data, the requester may give identification information of the recipient. The identification information may include a cell phone number of the recipient, an email address of the recipient, or any other information identifying the recipient. The computing device **1610** can send a message to the recipient by email, by text message, or by any other communication method. The message can include an indication to the recipient that card data is available for download and instructions on how the recipient can download the card data. When the recipient follows the download instructions, computing device **1630** is identified by computing device **1610** and the card data is delivered from computing device **1610** to computing device **1630**. In yet another example, the delivery of card data can take place via a social network. The requester may indicate a user name or other identifier of a contact in a social network as the recipient. A message can be sent to the recipient via the social network or post a message on a page associated with the recipient. The message can include an indication to the recipient that card data is available for download and instructions on how the recipient can download the card data. When the recipient follows the download instructions, computing device **1630** is identified by computing device **1610** and the card data is delivered from computing device **1610** to computing device **1630**. Any number of other examples of delivering data from computing device **1610** to computing device **1630** are possible.

Either or both of computing device **1630** and universal card **1640** can include a secure element. When computing device **1630** receives card data from the computing device **1610**, it can store the card data in either a secure element of the computing device **1630**, in a secure element of universal card **1640**, or in secure elements of both the computing device **1630** and the universal card **1640**. Once the card data is stored in a secure element, the universal card **1640** can be programmed to emulate a physical traditional card associated with the card data. It is also possible for card data to be stored in memory that is not part of a secure element. It may be advantageous to store card data associated with non-financial cards, such as loyalty cards, in memory that is outside of the secure element. Doing so may preserve limited memory capabilities of a secure element, leaving memory available in the secure element to store card data which cannot be stored outside of the secure element, such as bank card data.

The request for card data may be sent from computing device **1630**. In this embodiment, a user of computing device **1630** can request card data be sent to the user's own computing device **1630**. Computing device **1630** can be a cell phone, a PDA, an iPod, a tablet computer, a laptop computer, a desktop computer, an NFC-specialized device, or any other type of computing device. For example, the user may wish to add a loyalty card to the list of possible cards that the universal card **1640** can emulate. In this case, the user can contact the loyalty card issuer using computing device **1630**. Computing device **1630** can include any one of the following features which would allow the user to request card data: an e-wallet application, a card requesting application that is specifically dedicated to allowing users to request various types of card data, a retailer application that allows the user to request card data for that particular retailer, and a web browser that allows the user to access a website which allows the user to request card data. In one embodiment, the user of computing device **1630** may use an e-wallet application to request new card data. In this embodiment, the user could purchase a gift card using the e-wallet application on computing device **1630** and the remote computer **1620** could receive the request, process the purchase, and send card data for the gift card back to computing device **1630**. Using the e-wallet application to purchase the gift card allows the user to select any of the cards already stored in the e-wallet application to use for purchasing the gift card. Other methods and applications are available to allow a user to request card data.

The request for card data may be sent from a computing device **1650** that is different from computing device **1630**. In this embodiment, the requesting user may use any computing device **1650** which is capable of communicating a request for card data to computing device **1610**. Computing device **1650** can be a cell phone, a PDA, an iPod, a tablet computer, a laptop computer, a desktop computer, an NFC-specialized device, or any other type of computing device. For example, the requesting user may wish to send a gift card to the user of computing device **1630** in electronic format so that the recipient can use the universal card **1640** to emulate the gift card. In this case, the requesting user can contact the gift card issuer using computing device **1650**. In yet another example, a user can use one computing device **1650**, such as a laptop computer or desktop computer, to request that card data be sent to the user's own computing device **1630**, such as the user's tablet computer. Computing device **1650** can include any one of the following features which would allow the user to request card data: an e-wallet application, a card requesting application that is specifically dedicated to allowing users to request various types of card data, a retailer application that allows the user to request card data for that particular retailer, and a web browser that allows the user to access a website which allows the user to request card data.

The operator of computing device **1610** can be any number of entities. In one example, the operator of computing device **1610** can be a retailer. The retailer may operate a website through which a user can purchase products and gift cards specific to the retailer. The retailer may allow a user to purchase a gift card with delivery being in electronic form to the computing device **1630**. In this case, no physical card would be sent to the requester and/or the recipient; instead, card data would be delivered from computing device **1610** to computing device **1630** and the recipient would be able to program universal card **1640** to emulate a physical gift card. In another example, the operator of computing device **1610** can be a retailer which offers loyalty cards and/or membership cards.

The retailer may allow a user to request a loyalty card or purchase a membership card with delivery being in electronic form to the computing device **1630**. In this case, no physical loyalty card or membership card would be sent to the recipient because the universal card **1640** would be able to emulate a loyalty card or membership card. In another example, the operator of computing device **1610** can be a card issuer. A card issuer may allow a user to apply for a credit card. Upon approval of the credit card, the computing device **1610** can send card data to the computing device **1630** and the recipient would be able to program universal card **1640** to emulate a physical credit card. In yet another example, the operator of computing device **1610** can be a card issuer which allows users to purchase pre-paid debit cards. The card issuer may allow a user to purchase a pre-paid gift card with delivery being in electronic form to the computing device **1630**. In this case, no physical pre-paid debit card would be sent to the recipient; instead, card data would be delivered from computing device **1610** to computing device **1630** and the recipient would be able to program universal card **1640** to emulate a pre-paid debit card.

In the pre-paid debit card example, the ability to request and have pre-paid debit card data delivered to a recipient electronically could obviate the need for money wiring services. In one embodiment, a parent of a college student may wish to send money to the college student. Instead of using a money wiring service, the parent may use a computing device **1650** to contact a pre-paid debit card issuer and request that a pre-paid debit card be electronically delivered to the college student's computing device **1630**. Upon approval of the pre-paid debit card, the computing device **1610** can electronically deliver card data associated with the pre-paid debit card to the college student's computing device **1630**. Once the card data has been electronically delivered to computing device **1630**, the college student can use the pre-paid debit card by programming the universal card **1640** to emulate the pre-paid debit card. In this example, the parent was able to make money available to the college student without having to use a money wiring service and without having to ship a physical card to the college student.

The ability to send card data electronically can also improve customer loyalty reward systems. Some retailers reward customers for making purchases with loyalty cards in the form of gift cards, gift certificates, electronic gift certificates, and the like. Examples include retailers that send a gift card to customers once the customers reach some spending threshold and retailers that send electronic gift certificates to customers each month based on the amount customers have spent during the month. These systems require either that a physical gift card or gift certificate be sent to customers, or that customers print electronic gift certificates and physically bring the printed gift certificate to the retail location. Instead, if a customer has a universal card, the customer may be able to choose to receive all benefits in the form of electronic card data. In the example where a retailer normally provides a gift card once a customer reaches some spending threshold, the retailer could send gift card data to the customer's computing device for use with the customer's universal card. Similarly, in the example where a retailer normally provides an electronic gift certificate to a customer each month based on the amount the customer has spent during the month, the retailer could send gift card data to the customer's computing device for use with the customer's universal card. In another embodiment, the retailer may be aware that the customer already has both loyalty card data for that retailer and gift card data for that retailer available for use with the universal card. In this embodiment, when the retailer is due to send a gift card or a gift certificate to the customer, the retailer may instead credit the gift card account for which the user already has the gift card data and notify the customer that the gift card account has been credited with a certain amount.

The ability to send card data electronically without having a physical card can also reduce card fraud. One way in which fraud occurs is when a thief goes to a retail location where gift cards or other cards on displayed on shelves and records the information from not-yet-activated card, sometimes referred to as "skimming." The information can include a card number, a security or access code, and the like which are sometimes concealed by cardboard or a scratch off film. The thief monitors the card status online using the card information. Once the thief finds that the card has been activated, the thief depletes the value of the card before it is used. For example, with a gift card associated with a retailer, once the gift card has been activated, the thief can go to a website of the retailer and make a purchase using the gift card information. Skimming is eliminated if card data is sent electronically to a recipient and not available for inspection in physical form.

The above description of FIG. **16** refers to computing device **1610** as a single computing device. While computing device **1610** can be a single computer, it is important to note that computing device **1610** can include multiple computing devices, such as a number of servers, multiple data centers, and the like. Computing device **1610** can also be a point of sale terminal or terminals. In this embodiment, a point of sale terminal **1610** can send card data to a computing device **1630**. The gift card data can be transmitted from point of sale terminal **1610** to computing device **1630** via a network **1620**, such as a wi-fi network provided by the retailer. In one example, a user of computing device **1630** may be returning an item at the point of sale terminal **1610** and, in exchange for the return of the item, the user is entitled to a gift card with a certain amount of value. Instead of a cashier providing the user with a physical gift card, the point of sale terminal **1610** can send gift card data to the computing device **1630** where the gift card data is associated with a gift card account and is usable by the universal card **1640** to emulate the gift card. In another example, a user of computing device **1630** may wish to obtain a loyalty card while checking out at point of sale terminal **1610**. Instead of a cashier providing the user with a physical loyalty card, the point of sale terminal **1610** can send loyalty card data to the computing device **1630** where the loyalty card data is usable by the universal card **1640** to emulate the loyalty card.

Referring now to FIG. **17**, depicted is a method of providing card data to a universal card. A requester can send a request for card data to be sent to a recipient, as depicted by box **1710**. As discussed above, the requester can send the request from a computing device to one or more computing devices associated with the card distributor via a network. In addition, the computing device used by the requester can, but need not be, associated with a universal card. The request can optionally include information identifying the recipient or the recipient's computing device. The card distributor can receive the request for card data, as depicted by box **1720**. As discussed above, the request can be received by one or more computing devices associated with the card distributor via a network. The card distributor can identify a computing device associated with the recipient, as depicted by box **1730**. As discussed above, identifying the recipient's computing device can include sending an email or text message to the recipient with instructions for downloading the card data. The instructions can include actions by the recipient that will identify the recipient's computing device to the card distributor. Identifying the recipient's computing device can also

include information identifying the recipient's computing device in the request sent by the requester. In addition, as described above, the requester can also be the recipient. After the card distributor identifies the computing device of the recipient, the card distributor can deliver the card data to the recipient's computing device, as depicted by box **1740**. As described above, the delivery can be from one or more computing devices of the card distributor to the recipient's computing device via a network. The recipient's computing device can receive the card data and store the card data in a secure element. As describe above, the secure element can be located in one or both of the recipient's computing device or a universal card associated with the recipient's computing device. The recipient can program the universal card to emulate a card using the card data delivered to the computing device associated with the recipient.

Referring now to FIG. **18**, depicted are embodiments of a system and method of securely loading card data onto a universal card that has a secure element. In addition to those advantages discussed above, there are advantages to having the secure element on the universal card instead of the mobile device. A wireless carrier may assert control over access, management, and ownership of a secure element on a mobile device. Such control over the secure element may also include control over use of a short range transceiver for payments. Mobile device manufacturers and application developers can attempt to secure applications using other forms of security, such as secure elements located on SIM cards or SD cards. However, any application or data stored in a mobile device, a SIM card, or an SD card leaves the application or data susceptible to extraction, access, or inspection by thieves and/or hackers. The data on mobile devices can be read by third parties if the mobile device is lost or stolen. Users may protect their mobile device with a PIN or password; however, users frequently use only four-digit PIN numbers (a total of 10,000 possible PINs) or weak passwords that are easily overcome. If any secure card data is located on the phone, recovery of such data would allow the third party to complete transactions using the recovered phone data. Mobile devices also suffer from hacking attacks, such as phishing, Trojan, and Bot attacks. In a phishing attack, a mobile device's browser may be directed to phishing site which is configured to extract secure data from the phone or from the phone's user. In a Trojan or Bot attack, a mobile device may become infected with code which establishes a connection to a hacker's computing device and transfers secure data from the mobile device. Many other attacks on mobile devices are possible. Other attacks on mobile devices include intercepting data that is transmitted to other devices, sometimes referred to as "man-in-the-middle" attacks. When a device establishes a wireless connection, such as an NFC connection, a Bluetooth connection, or Wi-Fi connection, a third party may intercept signals sent via the wireless connection and read, modify, or reroute the data.

The system depicted in FIG. **18** prevents unencrypted secure card data from being stored on a mobile device and from being transmitted between devices. As depicted, encrypted card data **1810** can be sent to mobile device **1820**. In one embodiment, the card data can be encrypted using a derived unique key per transaction (DUKPT) key management encryption scheme. In such a scheme, a one-time unique encryption key can be derived for each transaction, and the key can be generated from a master base derivation key (BDK) shared by both the encrypting entity and the decrypting entity. In one embodiment, a unique BDK can be assigned to each customer. After receiving the encrypted card data **1810**, the mobile device **1820** can store the encrypted card data **1810**. The encrypted data **1810** can be stored either temporarily or indefinitely without concern for the mobile device **1820** being hacked, stolen, or otherwise compromised, as the encrypted card data **1810** can be encrypted in such a way that it is difficult or nearly impossible for the card data to be decrypted by a third party that does not have the proper key(s), such as the DUKPT and the BDK. Mobile device **1820** can include an e-wallet application **1821** and a short range transceiver **1822**. The encrypted card data **1810** is unusable to the e-wallet application **1821** since the e-wallet application **1821** is unable to decrypt the encrypted card data **1810**.

The mobile device **1820** can transmit the encrypted card data **1810** via the short range transceiver **1822** to universal card **1830** which also has a short range transceiver **1831**. While the transmission of the encrypted card data **1810** may be made wirelessly, such as via an NFC connection, a Bluetooth connection, or other short range communication connection, such a transmission will not expose the card data to risk of being read by a man-in-the-middle attack because the card data is being transmitted as encrypted card data **1810**. Even if the encrypted card data **1810** was read by a third party, it is difficult or nearly impossible for the card data to be decrypted by the intercepting party without the proper key(s). Once received via the short range transmitter **1831**, the encrypted card data **1810** can be passed to secure element **1832** on the universal card **1830**. The secure element **1833** can include a decrypting module **1833** which has sufficient information, such as the DUKPT and/or the BDK, to decrypt the card data. The decrypted card data can include both secure card data **1840** and non-secure card data **1850**. The secure card data can include information that is typically used to ensure security of financial transactions. For example, many traditional credit and debit cards include a card certification value (CVV1) that is encoded on Track 2 of the magnetic stripe of a traditional card. During a transaction, the CVV1 value is passed to the terminal with the other card data and the terminal can verify the transaction using the CVV1 value. In the system depicted in FIG. **18**, the decrypted secure card data **1840** could include the CVV1 value for a particular card. The secure card data **1840** is stored in the secure element **1832** of the universal card **1830**. The universal card **1830** can be configured so that it uses the secure card **1840** to configure dynamic magnetic stripe **1860** to emulate a static magnetic stripe of a traditional card, and the universal card **1830** can be configured so that the secure card data **1840** is stored only in secure element **1832** and not transmitted after the secure card data **1840** is decrypted. Non-secure card data **1850** can include information related to a card that would be considered acceptable if lost or stolen. Such non-secure data could include any or all of the following: the name of the issuer of the card (e.g., VISA, AMERICAN EXPRESS, etc), the name of the card holder, the last four digits of the card number, and the expiration date of the card.

The universal card **1830** can transmit the decrypted non-secure card data **1850** to the mobile device **1820** via short range transceiver **1831**. The decrypted non-secure card data **1850** can be sent to the mobile device **1820** in a batch file that can include non-secure card data for one or more cards. The mobile device **1820** can receive the non-secure card data **1850** via short range transceiver **1822** and store the non-secure card data **1850**. Once stored in the mobile device **1820** stores the non-secure card data **1850**, it can be used by e-wallet application **1821**. E-wallet application **1821** can provide a user interface which allows a user to view the non-secure card data **1850**, to manage card data and card accounts, to select a card for the universal card **1830** to emulate, to assign a nickname to a card, to assign an identifier of the type of card (e.g., VISA

word account, MASTERCARD home account, etc), choose a type of card (e.g., loyalty card, debit card, credit card), among other operations.

The system and method depicted in FIG. **18** provide a trusted environment for the secure card data **1840** and the decryption keys required for decrypting encrypted card data **1810**. Using the secure element **1832** on a universal card **1830** to both decrypt encrypted card data **1810** and to store decrypted secure card data **1840** greatly reduces the possibility of fraud or theft of card data. The secure card data **1840** does not need to be transmitted off of universal card **1830** and will not be available in a decrypted form off of universal card **1830**. Furthermore, mobile device **1820** will not contain any secure card data **1840** in a decrypted format. Thus, there will be no risk to the loss or theft of secure card data **1840** if mobile device **1820** is lost, stolen, or hacked.

Referring now to FIGS. **19**A-**19**C, depicted are several embodiments of systems and methods for providing card encrypted to a mobile device for transmission to a universal card with a secure element. Depicted in FIG. **19**A is an encrypting card reader **1910**. A user can swipe a traditional card into encrypting card reader **1910** which will read the data from the traditional card's magnetic stripe and encrypt that data as the card data is read from the traditional card's magnetic stripe to create encrypted card data **1920**. In one embodiment, the encrypting card reader **1910** can use a triple data encryption standard (3DES) and DUKPT to encrypt the card data as it the data is read from the traditional card's magnetic stripe. In the embodiment depicted in FIG. **19**A, the encrypting card reader **1910** can be connected directly to mobile device **1930**. The connection between encrypting card reader **1910** and mobile device **1930** can be a wired connection, such as a cable connecting encrypting card reader **1910** to an audio jack of mobile device **1930**, or a wireless connection, such as via a Wi-Fi network. The encrypted card data **1920** can be communicated from the encrypting card reader **1910** to the mobile device **1930** which transmits the encrypted card data **1920** to universal card **1940**. Universal card **1940** can include a secure element **1941** which has a decryption module that can decrypt encrypted card data **1920** and store decrypted secure card data. Universal card **1940** can also transmit decrypted non-secure card data back to mobile device **1930**.

Depicted in FIG. **19**B is an embodiment where encrypting card reader **1910** is connected to a computing device **1950**. Computing device **1950** can be any computing device, such as a personal computer, a laptop computer, a tablet, and the like. A user can swipe a traditional card into encrypting card reader **1910** which will read the data from the traditional card's magnetic stripe and encrypt that data as the card data is read from the traditional card's magnetic stripe to create encrypted card data **1920**. The encrypting card reader **1910** can be connected to computing device **1950** via a wired connection, such as a universal serial bus (USB) connection, or a wireless connection, such as via a Wi-Fi network. The encrypted card data **1920** can be communicated from the encrypting card reader **1910** to the computing device **1950** which transmits the encrypted card data **1920** to mobile device **1930**. Mobile device **1930** can transmit the encrypted card data **1920** to universal card **1940**. Universal card **1940** can include a secure element **1941** which has a decryption module that can decrypt encrypted card data **1920** and store decrypted secure card data. Universal card **1940** can also transmit decrypted non-secure card data back to mobile device **1930**.

Depicted in FIG. **19**C is an embodiment where a source of encrypted card data **1960** provides encrypted card data **1920** to mobile device **1930**. The source of encrypted card data **1960** can be a financial institution, such as a bank, a card issuer, such as a credit card company, a point of sale terminal, such as a terminal in a store that issues loyalty cards and gift cards, or any other source of encrypted card data. The source of encrypted card data **1960** can encrypt the card data to create the encrypted card data **1920** and transmit the encrypted card data **1920** to mobile device **1930** via a network **1970**. The network **1970** can be a wired network, a wireless network, or any combination of wired and wireless networks, including one or more of the internet, a cellular phone network, a Wi-Fi network, a local area network, a wide area network, and the like. The network **1970** can also include one or more computing devices. For example, a bank may send encrypted card data **1920** to a user's personal computer via the internet, and the user's personal computer can send the encrypted card data **1920** to mobile device **1930** via a wireless connection, such as a Bluetooth connection or a Wi-Fi connection. In this example, the network **1970** would include the internet, the user's personal computer, and the wireless connection between the user's personal computer and the mobile device **1930**. Mobile device **1930** can transmit the encrypted card data **1920** to universal card **1940**. Universal card **1940** can include a secure element **1941** which has a decryption module that can decrypt encrypted card data **1920** and store decrypted secure card data. Universal card **1940** can also transmit decrypted non-secure card data back to mobile device **1930**.

The encryption of card data can be used with any type of traditional card data. For example, credit card data, debit card data, loyalty card data, identification card data, building access card data, and card data of any other type of card can be encrypted before it is sent to a universal card via a mobile device. The ability to send encrypted card data to a universal card via a mobile device does not preclude the possibility that card data could be sent to a universal card via a mobile device in an unencrypted form. In certain instances, it may be difficult to securely share decryption keys with a universal card. In such instances, it may be more advantageous to send card data in a decrypted form. For example, it may not be required that electronic gift card data is encrypted for transmission to the universal card, and it may be difficult to securely pass decryption keys to the universal card from every possible retailer, electronic gift card issuer, social media site, etc., that issues electronic gift cards. Thus, it may be advantageous to transmit electronic gift card data to a universal card via a mobile device in an unencrypted format even if all other types of card data, such as credit card data, is transmitted to the universal card via the mobile device in an encrypted format.

Referring now to FIG. **20**, depicted is an embodiment of a method of securely transferring secure card data to a universal card and non-secure card data to a mobile device. At block **2010**, the card data is encrypted. In some embodiments, the encryption can be performed by a card issuer, a financial institution, an encrypting card reader, and the like. At block **2020**, the encrypted card data is transmitted to a mobile device. The transmission can be performed via one or both of a wired connection and a wireless connection. At block **2030**, the mobile device stores the encrypted card data. At block **2040**, the mobile device transmits the encrypted card data to a universal card. In one embodiment, the transmission to the universal card is done via a short range communication link, such as an NFC communication link or a Bluetooth communication link. At block **2050**, a secure element of the universal card decrypts the encrypted card data. The decrypted card data can include both secure card data and non-secure card data. As shown at block **2050**, the secure element can also store the decrypted secure card data. At block **2060**, the universal card transmits the decrypted, non-secure card data to

the mobile device. In one embodiment, the transmission to the mobile device is done via a short range communication link, such as an NFC communication link or a Bluetooth communication link. At block **2070**, an e-wallet application on the mobile device stores the decrypted non-secure card data. While the blocks depicted in FIG. **20** show an order to the steps, one of ordinary skill in the art would recognize that at least some of the steps could be performed in a different order and the methods described herein are not limited to only the order depicted in FIG. **20**.

Referring now to FIGS. **21**A and **21**B, depicted are embodiments of a mobile device obtaining and using RF card data in conjunction with a universal card. FIG. **21**A depicts a mobile device **2110** which has a short range transceiver **2111** and an e-wallet application **2112**. FIG. **21**A also depicts a contactless traditional card **2120** which has an RF interface **2121**. The RF interface **2121** transmits encrypted RF card data **1930**. Some point-of-sale terminals have contactless payment terminals where an RF receiver can receive the encrypted RF card data **1930** as part of a contactless payment transaction. In such a transaction, a card holder merely brings the contactless traditional card **2120** in close proximity to the contactless payment terminal at which time the encrypted RF card data **1930** is passed from the RF interface **2121** to the contactless payment terminal. In the embodiment depicted in FIG. **21**A, the contactless traditional card **2120** can be brought in close proximity to or tapped to the mobile device **2110** when the mobile device is acting as a contactless payment terminal so that the encrypted RF card data **1930** is transmitted from the RF interface **2121** and received by the short range transceiver **2111** of the mobile device **2110**. The mobile device **2110** can store the encrypted RF card data **1930** for later use. Since the encrypted RF card data **1930** is already fully encrypted, no further encryption is needed to protect the encrypted RF card data **1930**.

The mobile device **2110** may also store non-secure card data associated with the RF-enabled traditional card **2120**. In one embodiment, such non-secure card data can be received from a universal card which decrypts encrypted card data. More specifically, in accordance with the description above, the contactless traditional card **2120** may also have a static magnetic stripe which can be read by an encrypting card reader which transmits encrypted card data to the mobile device **2110**. The mobile device **2110** can transmit the encrypted card data to a universal card which has a secure element with a decrypting module that decrypts the encrypted card data to obtain decrypted secure card data and decrypted non-secure data. The universal card can transmit the decrypted non-secure card data to the mobile device **2110** which can receive and store the decrypted non-secure data. The mobile device **2110** includes an e-wallet application **2112** which can be used to manage all of the various types of card data on the mobile device **2110**. In one embodiment, the e-wallet application can be used to associate the encrypted RF card data **1930** and the non-secure card data stored on the mobile device **2110** with a single card account. For example, a user could associate encrypted RF card data **1930** and the non-secure card data stored with a card account having a nickname of "Work VISA."

Referring now to FIG. **21**B, depicted is a an embodiment of the actions taken by the mobile device **2110** when a particular card is selected. Using the e-wallet application **2112** on mobile device, a user can associate both encrypted RF card data **1930** and non-secure card data with a single card account. When the user wants to make a payment, the user can select the card account in the e-wallet application **2112**. Upon receiving the user selection of a card account, the e-wallet application **2112** can send encrypted RF card data **1930** and an indication of the selected card **1940** to the short range transceiver **2111**. The short range transceiver **2111** can use the encrypted RF card data **1930** such that the mobile device can be presented at a contactless payment terminal **2170**. In this case, the mobile device **2110** acts as a contactless payment card. If universal card **2150** is in proximity to the mobile device **2110** to establish a short range communication link, the indication of the selected card **1940** is sent to a short range transceiver **2151** of universal card **2150**. The universal card **2150** includes a secure element **2152** which can store secure card data **2160** which is usable to configure a dynamic data communication mechanism, such as a dynamic magnetic stripe, of the universal card **2150**. Upon receiving the indication of the selected card **1940**, the universal card can configure the dynamic data communication mechanism to emulate a static data communication mechanism of a traditional card. For example, if the dynamic data communication mechanism is a dynamic magnetic stripe, the universal card **2150** can be presented to a magnetic stripe payment terminal **2180** after the dynamic magnetic stripe is configured to emulate a static magnetic stripe of a traditional card. In the embodiment depicted in FIG. **21**B, the user's selection of a single card account, such as the "Work VISA" nicknamed account from the example in the preceding paragraph, in the e-wallet application will enable the user to make a payment from the "Work VISA" account either using the mobile device itself with a contactless payment transaction terminal or using the dynamic data communication mechanism of the universal card if the universal card is in close enough proximity to receive the indication of the selected "Work VISA" card. Such a system can lower the complexity of making a payment for the user as the user can make a payment using either the mobile device or the universal card after making a single selection of the card account.

Referring now to FIGS. **22**A, **22**B, and **22**C, depicted is an embodiment of a universal card with a dynamic EMV chip. A front of universal card **2200** is depicted in FIG. **22**A with a dynamic EMV chip **2201**. The dynamic EMV chip **2201** is configurable to emulate any number of static EMV chips. One embodiment of a back of universal card **2200** is depicted in FIG. **22**B with a dynamic magnetic stripe **2202**; however, a dynamic magnetic stripe **2202** is not required to be on a universal card **2200** that has a dynamic EMV chip **2201**. Other items not picture in FIG. **22**A or **22**B can be located on the front or back of universal card **2200**, such as a signature bar, the name of a user of the universal card, a display, a power indicator, a switch, a branding area, and other items.

One embodiment of a secure element **2203** inside of universal card **2200** is depicted in FIG. **22**C. Secure element **2203** can store EMV card data **2204** for any number of EMV cards. As depicted in FIG. **22**C, secure element **2203** includes EMV card data $\mathbf{2204}_1$ for a first card, $\mathbf{2204}_2$ for a second card, and $\mathbf{2204}_N$ for an nth card. The EMV card data **2204** for each card can include any or all of the EMV card data needed to execute both online and offline transactions, such as security credentials, cryptographic keys, DDA data, SDA data, CDA data, and cardholder verification data. The EMV card data **2204** for each card can also include and data necessary for using the EMV card in an EMV contactless transaction or an EMV contact transaction. Storing EMV card data **2204** in secure element **2203** ensures that the EMV card data **2204** cannot be extracted from universal card **2200**, reducing the possibility of fraud. The EMV card data **2204** for each card can be compartmentalized and stored in separate memory blocks in secure element **2203**, as is shown with respect to EMV card data $\mathbf{2204}_1$, EMV card data $\mathbf{2204}_2$, and $\mathbf{2204}_N$.

Storing EMV card data **2204** for each card in separate memory blocks in secure element **2203** ensures that the EMV card data **2204** for one card remains isolated from any other card's credentials and maintains the security and data integrity of the EMV card data **2204** for each card. The secure element **2203** can optionally include other functionality or data, such as magnetic stripe data **2205** of one or more card accounts, card manager **2206**, and card data decrypter **2007**.

EMV card data can be stored in a universal card in a number of ways. In one embodiment, EMV card data can be loaded on to a universal card by the issuer of the universal card prior to the universal card being issued to the user of the universal card. For example, if a bank issues the universal card to a user, the bank could store EMV card data for any card issued by the bank, such as a bank-issued debit card, a bank-issued debit card, etc., on the universal card before the bank issued the universal card to the user. In another embodiment, depicted in FIG. **23**A, a trusted source **2301** can transmit encrypted EMV card data **2302** via a network **2303** to a computing device **2304**. Attached to the computing device **2304** is an EMV card reader/writer **2305** which can interface with an EMV chip on a universal card **2306**. The computing device **2304** can write the encrypted card data **2302** to the universal card **2306** using the EMV card reader/writer **2305**. In another embodiment, depicted in FIG. **23**B, a trusted source **2311** can transmit encrypted EMV card data **2312** via a network **2313** to a computing device **2314**. The computing device **2314** can be configured to communicate the encrypted EMV card data **2312** to a universal card **2315**. The encrypted EMV card data **2312** can be communicated from computing device **2314** to universal card **2315** via a wired connection, such as via a USB or other serial connection, or via a wireless connection, such as an NFC communication link, a Bluetooth communication link, or other short range communication link.

Referring now to FIG. **24**, depicted is an embodiment of a method of handling encrypted EMV card data by a computing device and a universal card. At block **2410**, the EMV card data is encrypted. In some embodiments, the encryption can be performed by a trusted source, such as a card issuer, a financial institution, an encrypting card reader, and the like. At block **2420**, the encrypted EMV card data is transmitted to a computing device. The transmission can be performed via one or both of a wired connection and a wireless connection. At block **2430**, the computing device stores the encrypted EMV card data. At block **2440**, the computing device transmits the encrypted EMV card data to a universal card. In one embodiment, the transmission to the universal card is done via a short range communication link, such as an NFC communication link or a Bluetooth communication link. At block **2450**, a secure element of the universal card decrypts the encrypted EMV card data. The decrypted EMV card data can include both secure EMV card data and non-secure EMV card data. As shown at block **2450**, the secure element can also store the decrypted EMV secure card data. At block **2460**, the universal card transmits the decrypted, non-secure EMV card data to the computing device. In one embodiment, the transmission to the computing device is done via a short range communication link, such as an NFC communication link or a Bluetooth communication link. At block **2470**, an e-wallet application on the computing device stores the decrypted, non-secure EMV card data. While the blocks depicted in FIG. **24** show an order to the steps, one of ordinary skill in the art would recognize that at least some of the steps could be performed in a different order and the methods described herein are not limited to only the order depicted in FIG. **24**.

Using an e-wallet application on the computing device, a user can instruct the dynamic EMV chip of the universal card to emulate a static EMV chip using the EMV card data stored in the secure element. When the user wants to make a payment, the user can select the EMV card account in the e-wallet application. Upon receiving the user selection of a card account, the e-wallet application can send an indication of the selected EMV card to a short range transceiver. The short range transceiver can send the indication of the selected EMV card to a short range transceiver of the universal card. The universal card can use the EMV card data stored in the secure element to configure a dynamic EMV chip of the universal card to emulate a static EMV chip. For example, the universal card can be presented to an EMV payment terminal after the dynamic EMV chip is configured to emulate a static EMV chip. The universal card would then act as a traditional EMV card to carry out the transaction with the EMV terminal. In one embodiment, the universal card could carry out either an online or an offline EMV transaction with the EMV terminal.

The above includes descriptions of a mobile device and a universal card. A mobile device can be any computing device, such as a mobile phone, a Personal Digital Assistants (PDA), an iPod, an MP3 player, a tablet computer, a laptop computer, a personal computer and similar mobile devices. Any of these mobile devices can have short range communication mechanisms, such as a NFC transceiver or a Bluetooth transceiver, which permits the mobile device to communicate with a universal card.

The various techniques described herein may be implemented with hardware or software or, where appropriate, with a combination of both. Thus, the methods and apparatus of the disclosed embodiments, or certain aspects or portions thereof, may take the form of program code (i.e., instructions) embodied in tangible media, such as floppy diskettes, CD-ROMs, hard drives, or any other machine-readable storage medium. When the program code is loaded into and executed by a machine, such as a computer, the machine becomes an apparatus for practicing the disclosed embodiments. In the case of program code execution on programmable computers, the computer will generally include a processor, a storage medium readable by the processor (including volatile and non-volatile memory and/or storage elements), at least one input device and at least one output device. One or more programs are preferably implemented in a high level procedural or object oriented programming language to communicate with a computer system. However, the program(s) can be implemented in assembly or machine language, if desired. In any case, the language may be a compiled or interpreted language, and combined with hardware implementations.

The foregoing description has set forth various embodiments of the apparatus and methods via the use of diagrams and examples. While the present disclosure has been described in connection with the preferred embodiments of the various figures, it is to be understood that other similar embodiments may be used or modifications and additions may be made to the described embodiment for performing the same function of the present disclosure without deviating there from. Therefore, the present disclosure should not be limited to any single embodiment, but rather construed in breadth and scope in accordance with the appended claims. Additional features of this disclosure are set forth in the following claims.

What is claimed:

1. A method of handling EMV (Europay, MasterCard and Visa) card data, the method comprising:

receiving, by a computing device, EMV card data in an encrypted format;

transmitting, from the computing device to a universal card, the EMV card data in the encrypted format, wherein the universal card comprises a secure element which is configured to decrypt the EMV card data, and wherein the universal card is configured to store the decrypted EMV card data in the secure element;

receiving, by the computing device from the universal card, non-secure EMV card data;

storing, in the computing device, the non-secure EMV card data, wherein the computing device comprises an e-wallet application, the e-wallet application permitting a user selection of an EMV card based on an identification of at least a portion of the non-secure EMV card data;

sending, from the computing device to the universal card, an indication of the selected card, wherein the universal card is configured to configure a dynamic EMV chip of the universal card; and

emulating a static EMV chip of the selected card using at least a portion of the decrypted EMV card data stored in the secure element of the universal card.

2. The method of claim **1**, wherein transmitting, from the computing device to the universal card, the EMV card data in the encrypted format comprises transmitting the EMV card data in the encrypted format via a short range transceiver of the computing device.

3. The method of claim **1**, further comprising:

storing, by the computing device, the EMV card data in the encrypted format after receiving the EMV card data in the encrypted format.

4. The method of claim **1**, wherein receiving the EMV card data in the encrypted format comprises receiving, by the computing device, the EMV card data in the encrypted format from a trusted source.

5. The method of claim **1**, wherein receiving the EMV card data in the encrypted format comprises receiving, by the computing device, the EMV card data in the encrypted format via a network.

6. The method of claim **1**, wherein the EMV card data comprises one or more of gift card data, prepaid card data, and stored value card data, and wherein the selected card is associated with one of the gift card data, the prepaid card data, and the stored value card data.

7. A non-transitory computer readable medium having instructions embodied thereon for handling EMV (Europay, MasterCard and Visa) card data, the instructions, when executed by a computing device, causing the computing device to:

receive, by the computing device, EMV card data in an encrypted format;

transmit, from the computing device to a universal card, the EMV card data in the encrypted format, wherein the universal card comprises a secure element which is configured to decrypt the EMV card data, and wherein the universal card is configured to store the decrypted EMV card data in the secure element;

receive, by the computing device from the universal card, non-secure EMV card data;

store, in the computing device, the non-secure EMV card data, wherein the computing device comprises an e-wallet application configured to permit a user selection of an EMV card based on an identification of at least a portion of the non-secure EMV card data; and

send, from the computing device to the universal card, an indication of the selected card, wherein the universal card is configured to configure a dynamic EMV chip of the universal card, wherein the dynamic EMV chip emulates a static EMV chip of the selected card using at least a portion of the decrypted EMV card data stored in the secure element of the universal card.

8. The non-transitory computer readable medium of claim **7**, wherein the instructions to transmit, from the computing device to the universal card, the EMV card data in the encrypted format comprise instructions to transmit the EMV card data in the encrypted format via a short range transceiver of the computing device.

9. The non-transitory computer readable medium of claim **7**, the instructions further comprising:

instructions to store, by the computing device, the EMV card data in the encrypted format after receiving the EMV card data in the encrypted format.

10. The non-transitory computer readable medium of claim **7**, wherein the instructions to receive the EMV card data in the encrypted format comprise instructions to receive, by the computing device, the EMV card data in the encrypted format from a trusted source.

11. The non-transitory computer readable medium of claim **7**, wherein the instructions to receive the EMV card data in the encrypted format comprise instructions to receive, by the computing device, the EMV card data in the encrypted format via a network.

12. The non-transitory computer readable medium of claim **7**, wherein the EMV card data comprises one or more of gift card data, prepaid card data, and stored value card data, and wherein the selected card is associated with one of the gift card data, the prepaid card data, and the stored value card data.

13. A computing device comprising:

a short range transceiver;

an e-wallet application; and

a computer readable medium having instructions embodied thereon, the instructions comprising instructions that, when executed by the computing device, cause the computing device to:

receive EMV (Europay, MasterCard and Visa) card data in an encrypted format;

transmit, to a universal card via the short range transceiver, the EMV card data in the encrypted format, wherein the universal card comprises a secure element which is configured to decrypt the EMV card data, and wherein the universal card is configured to store the decrypted EMV card data in the secure element;

receive, from the universal card, non-secure EMV card data;

store the non-secure EMV card data, wherein the e-wallet application is configured to permit a user selection of a card based on an identification of at least a portion of the non-secure EMV card data; and

send to the universal card an indication of the selected card, wherein the universal card is configured to configure a dynamic EMV chip of the universal card, wherein the dynamic EMV chip emulates a static EMV chip of the selected card using at least a portion of the decrypted EMV card data stored in the secure element of the universal card.

14. The computing device of claim **13**, the instructions further comprising:

instructions to store the EMV card data in the encrypted format after receiving the EMV card data in the encrypted format.

15. The computing device of claim **13**, wherein the instructions to receive the EMV card data in the encrypted format comprise instructions to receive the EMV card data in the encrypted format from a trusted source.

16. The computing device of claim 13, wherein the instructions to receive the EMV card data in the encrypted format comprise instructions to receive the EMV card data in the encrypted format via a network.

17. The computing device of claim 13, wherein the EMV card data comprises one or more of gift card data, prepaid card data, and stored value card data, and wherein the selected card is associated with one of the gift card data, the prepaid card data, and the stored value card data.

18. A method of handling EMV (Europay, MasterCard and Visa) card data, the method comprising:

receiving, by a universal card from a computing device, EMV card data in an encrypted format;

decrypting, by a decrypting module in a secure element of the universal card, the EMV card data;

storing the decrypted EMV card data in the secure element of the universal card;

transmitting, by the universal card to the computing device, non-secure EMV card data, wherein the computing device comprises an e-wallet application, the e-wallet application permitting a user selection of an EMV card based on an identification of at least a portion of the non-secure EMV card data;

receiving, by the universal card from the computing device, an indication of the selected EMV card;

configuring a dynamic EMV chip of the universal card to emulate a static EMV chip of the selected card; and

emulating the static EMV chip of the selected card using at least a portion of the decrypted EMV card data stored in the secure element.

19. The method of claim 18, wherein receiving, by the universal card from the computing device, the EMV card data in the encrypted format comprises receiving the EMV card data in the encrypted format via a short range transceiver of the universal card.

20. The method of claim 18, wherein the computing device is configured to receive the EMV card data in the encrypted format from a trusted source.

21. The method of claim 18, wherein the computing device is configured to receive the EMV card data in the encrypted format via a network.

22. The method of claim 18, wherein the EMV card data comprises one or more of gift card data, prepaid card data, and stored value card data, and wherein the selected card is associated with one of the gift card data, the prepaid card data, and the stored value card data.

23. A non-transitory computer readable medium having instructions embodied thereon for handling card data, the instructions, when executed by a computing device, causing the computing device to:

receive, by a universal card from the computing device, EMV (Europay, MasterCard and Visa) card data in an encrypted format;

decrypt, by a decrypting module in a secure element of the universal card, the EMV card data;

store the decrypted EMV card data in the secure element of the universal card;

transmit, by the universal card to the computing device, non-secure EMV card data, wherein the computing device comprises an e-wallet application configured to permit a user selection of an EMV card based on an identification of at least a portion of the non-secure EMV card data;

receive, by the universal card from the computing device, an indication of the selected EMV card; and

configure a dynamic EMV chip of the universal card, wherein the dynamic EMV chip emulates a static EMV chip of the selected card using at least a portion of the decrypted EMV card data stored in the secure element.

24. The non-transitory computer readable medium of claim 23, wherein the instructions to receive, by the universal card from the computing device, the EMV card data in the encrypted format comprise instructions to receive the EMV card data in the encrypted format via a short range transceiver of the universal card.

25. The non-transitory computer readable medium of claim 23, wherein the computing device is configured to receive the EMV card data in the encrypted format from a trusted source.

26. The non-transitory computer readable medium of claim 23, wherein the computing device is configured to receive the EMV card data in the encrypted format via a network.

27. The non-transitory computer readable medium of claim 23, wherein the EMV card data comprises one or more of gift card data, prepaid card data, and stored value card data, and wherein the selected card is associated with one of the gift card data, the prepaid card data, and the stored value card data.

28. A universal card comprising:

a dynamic EMV (Europay, MasterCard and Visa) chip;

a secure element comprising a decrypting module; and

a computer readable medium having instructions embodied thereon, the instructions comprising instructions that, when executed by the universal card, cause the universal card to:

receive, from a computing device, EMV card data in an encrypted format;

decrypt, by the decrypting module, the EMV card data;

store the decrypted EMV card data in the secure element;

transmit, to the computing device, non-secure EMV card data, wherein the computing device comprises an e-wallet application configured to permit a user selection of an EMV card based on an identification of at least a portion of the non-secure EMV card data;

receive, from the computing device, an indication of the selected EMV card; and

configure the dynamic EMV chip, wherein the dynamic EMV chip emulates a static EMV chip of the selected card using at least a portion of the decrypted EMV card data stored in the secure element.

29. The universal card of claim 28, the universal card further comprising:

a short range transceiver, wherein the instructions to receive, from the computing device, the EMV card data in the encrypted format comprise instructions to receive the EMV card data in the encrypted format via the short range transceiver.

30. The universal card of claim 28, wherein the computing device is configured to receive the EMV card data in the encrypted format from a trusted source.

31. The universal card of claim 28, wherein the computing device is configured to receive the EMV card data in the encrypted format via a network.

32. The universal card of claim 28, wherein the EMV card data comprises one or more of gift card data, prepaid card data, and stored value card data, and wherein the selected card is associated with one of the gift card data, the prepaid card data, and the stored value card data.

* * * * *